



governmentattic.org

"Rummaging in the government's attic"

Description of document:	Federal Communications Commission (FCC) Directives, 2010-2017
Requested date:	January 2017
Released date:	30-March-2017
Posted date:	11-December-2017
Source of document:	Freedom of Information Act Request Federal Communications Commission 445 12th Street, S.W., Room 1-A836 Washington, D.C. 20554 FOIA Online

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



Federal Communications Commission
Washington, D.C. 20554

March 30, 2017

Re: FOIA Control No. 2017-312

This letter responds to your Freedom of Information Act (FOIA) request for a, "digital/electronic copy of each current FCC Directive." Your request has been assigned FOIA Control No. 17-312. We extended the deadline for response to March 14, 2017 and March 28, 2017 pursuant to Section 0.461(g)(1)(ii) of our rules.¹

The Office of the Managing Director conducted a search for responsive records and is providing all 33 FCC directives as you requested. The electronic copies are in a zip file attached to the email message accompanying this letter.

We are required by both the FOIA and the Commission's own rules to charge requesters certain fees associated with the costs of searching for, reviewing, and duplicating the sought after information.² To calculate the appropriate fee, requesters are classified as: (1) commercial use requesters; (2) educational requesters, non-commercial scientific organizations, or representatives of the news media; or (3) all other requesters.³

Pursuant to section 0.466(a)(8) of the Commission's rules, you have been classified for fee purposes as category (3), "all other requesters."⁴ As an "all other requester," the Commission assesses charges to recover the full, reasonable direct cost of searching for and reproducing records that are responsive to the request; however, you are entitled to be furnished with the first 100 pages of reproduction and the first two hours of search time without charge under section 0.470(a)(3)(i) of the Commission's rules.⁵ The production did not involve more than 100 pages of duplication and took less than two hours of search time. Therefore, you will not be charged any fees.

If you consider this to be a denial of your FOIA request, you may seek review by filing an application for review with the Office of General Counsel. An application for review must be *received* by the Commission within 90 calendar days of the date of this letter.⁶ You may file an application for review by mailing the application to Federal

¹ 47 C.F.R. § 0.461(g)(1)(ii).

² See 5 U.S.C. § 552(a)(4)(A), 47 C.F.R. § 0.470.

³ 47 C.F.R. § 0.470.

⁴ 47 C.F.R. § 0.466(a)(8).

⁵ 47 C.F.R. § 0.470(a)(3)(i).

⁶ 47 C.F.R. §§ 0.461(j), 1.115; 47 C.F.R. § 1.7 (documents are considered filed with the Commission upon their receipt at the location designated by the Commission).

Communications Commission, Office of General Counsel, 445 12th St SW, Washington, DC 20554, or you may file your application for review electronically by e-mailing it to FOIA-Appeal@fcc.gov. Please caption the envelope (or subject line, if via e-mail) and the application itself as “Review of Freedom of Information Action.”

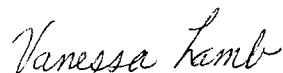
If you would like to discuss this response before filing an application for review to attempt to resolve your dispute without going through the appeals process, you may contact the Commission’s FOIA Public Liaison for assistance at:

FOIA Public Liaison
Federal Communications Commission, Office of the Managing Director,
Performance Evaluation and Records Management
445 12th St SW, Washington, DC 20554
202-418-0440
FOIA-Public-Liaison@fcc.gov

If you are unable to resolve your FOIA dispute through the Commission’s FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman’s office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road–OGIS
College Park, MD 20740-6001
202-741-5770
877-684-6448
ogis@nara.gov
ogis.archives.gov

Sincerely,

A handwritten signature in cursive script that reads "Vanessa Lamb".

Vanessa Lamb
Deputy Associate Managing Director
Office of Managing Director
Performance Evaluation and Records
Management – FOIA Program Office

Enclosures

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Policy for Use of Auction and Credit Reform Funds by the Federal Communications Commission	
	Directive Number: FCCINST 1006.2	Effective Date: July 2015

1. **PURPOSE:** This directive sets forth the Federal Communications Commission's (FCC or Commission) policies, procedures, and responsibilities relating to the availability, use, and apportionment of spectrum auction funds for necessary Commission auction program and credit reform program expenses. The principal intent of this document is to enable Fund Managers, Central Account Managers (CAM's), and personnel involved in the authorized obligation and use of auction and credit reform funds as well as those involved with internal auditing, financial tracking, training, and reporting to have a clear and concise understanding of the policies and procedures for the use of these funds. In addition, this directive provides instructions for requesting and obligating these funds.
2. **SCOPE:** This directive applies to all Bureaus and Offices within the FCC.
3. **AUTHORITY:** The Communications Act of 1934, Section 309(j).
4. **BACKGROUND:** The Omnibus Budget Reconciliation Act of 1993 added Section 309(j) to the Communications of Act 1934, as amended, which established the Commission's spectrum auction program. Among other things, section 309(j) gave the Commission express authority to employ competitive bidding procedures to choose among mutually exclusive applications for initial licenses. Section 309(j)(8) gave the Commission authority to use auction proceeds to fund the cost of developing and implementing the section 309(j) spectrum auction program. The uses of these funds are subject to the same legislative and budgetary controls as other Commission appropriations. This section was subsequently amended to authorize offsetting collections to remain available until expended. Additional requirements for reporting of auction's operating costs in the FCC Annual Report were contained in the Balanced Budget Act of 1997 (P.L. 105-33).

In addition, subsection 6403(c)(2)(C) of the Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96) directs the Commission authority to include in spectrum auction costs those incentive auction costs incurred by the Commission in conducting the reverse auction under subsection 6403(a)(1), conducting the evaluation of the broadcast television spectrum under subparagraph (A) of subsection 6403(b)(1), and making any reassignments or reallocations under subparagraph (B) of such subsection, in addition to

the costs incurred by the Commission in conducting the forward auction described in subsection 6403(c).

The Credit Reform Act of 1996 provided for every federal agency with debt management activities to report and manage the debt within certain guidelines, which are set forth in OMB Circular A-129. Additionally, Circular A-11 provides for agencies to obtain funding to accommodate certain reporting and managing activities associated with federal debt.

5. DEFINITIONS:

Appropriation. An authorization by act of Congress that permits Federal agencies to incur obligations and to make payments out of the Treasury for specified purposes. An appropriation follows enactment of authorizing legislation. Appropriations represent limitations on amounts that agencies may obligate during the time specified in the respective appropriation act.

Budget Object Classification Code (BOCC). Each category of expense required to support a responsible center or the activities supervised by a (CAM). BOCCs are used by the Federal government to record its financial transactions according to the nature of service provided or received at the time obligations are incurred.

Commission-wide. Referring to activities that benefit the entire Commission.

Cost Organization. A four-digit number that identifies the organization to which a commitment, obligation, disbursement, or receipt transaction applies.

Fund Manager or Central Account Managers (CAM). The Fund Manager or CAM is the individual within the organization charged with budgeting, reporting, and financial management of the expenses of a responsible center.

Obligation. A binding agreement that will require an outlay or expenditure of funds, immediately or in the future. Obligations may not be incurred unless the appropriate approval is secured prior to the transaction taking place.

Project Code. A five-digit alphanumeric code that identifies the activity to which a commitment, obligation, disbursement, or receipt transaction applies.

6. POLICY: Standard practices shall be established and followed at the FCC to ensure compliance with the auction expenditure provisions of Section 309(j) of the Communications Act of 1934, as amended and the Middle Class Tax Relief and Job Creation Act of 2012. In accordance with these Acts, spectrum auction and incentive auction proceeds may be retained by the FCC as an offsetting collection to defray Commission expenses associated with the development and implementation of the auction program as described in the paragraph below and Section 8, "Categories of Auction Cost Recovery and Credit Reform Funds Use." The amount of each expense is to be justified by the CAM requesting the funds.

If expenditures for equipment or services are necessary in order to develop and implement the auction program and the expenditure is justified as described in this directive, the total amount may be funded from available auctions offsetting collections. Similarly, if the expenditure for equipment or services will increase as a consequence of the auction program and the increased expenditure is cost justified, an appropriate portion of the cost of the equipment or service may be funded from available auctions offsetting collections. Thus, the Commission may retain auction proceeds as an offsetting collection and use them to defray the costs of:

- A. establishing and defending rules, orders or policies for the auction program, including any internal rules and policies;
- B. planning and executing the actual auctions;
- C. recording and reporting transfer of funds associated with auctions;
- D. awarding auctioned licenses;
- E. ensuring the legitimacy of applicants and winners who apply for special auction incentives;
- F. explaining operation of the auctions program, its implementing rules, and reporting on its progress to the public-at-large, potential bidders and Congress;
- G. conducting research, including economic experiments, using internal staff and external consultants, to develop, evaluate, and test alternative auction designs and formats;
- H. conducting post-auction activities to ensure integrity of the auctions program (i.e. performing audits, inspections, and investigations); and
- I. all other personnel and other costs incurred as a necessary result of the auction program, including those that provide support to employees, projects and systems Commission-wide.

In addition, if administration expenditures are necessary to maintain the credit reform program, and the expenditure is justified as described in this directive, the total amount may be funded from available credit reform appropriations. The Commission may retain credit reform appropriations for the following administrative expenditures:

- A. the appropriation of administrative expense that are shared with non-credit programs;
- B. the cost of loan systems development and maintenance, including computer costs;
- C. the cost of monitoring credit program and private lenders for compliance with laws and regulations;
- D. the cost of all activities related to credit extension, loan servicing, write-off, and close out;
- E. the cost of collecting delinquent loans, except for the cost of foreclosing, managing, and selling collateral that are capitalized or routinely deducted from the proceeds of sales;

- F. the costs of tracking regulatory requests, preparing decisional documents, and defending litigation relating to policies and rules governing the installment payment program for spectrum licenses assigned through competitive bidding;
- G. the costs related to offering at auction new licenses for spectrum associated with licenses that cancelled for non-payment of installment loans; and
- H. conducting credit reform activities to ensure integrity of the credit reform program (i.e. performing audits, inspections, and investigations).

7. RESPONSIBILITIES:

A. The Office of Managing Director (OMD) will:

Approve all Commission-wide requests for use of auction cost recovery and credit reform funds. Manage all aspects of budgetary and financial management of auction and credit reform funds.

B. The Chief Financial Officer (CFO) will:

1. Supervise and coordinate budgetary and financial management of the use of auction receipts to fund the auction program and the appropriation of funds to the credit reform programs.
2. Ensure that transactions are formulated and executed in accordance with the same federal rules and regulations that pertain to the Commission's appropriated funds.
3. Be responsible for approving all auction and credit reform fund justification related documentations that are originated from bureau or office.
4. Approve the use of auctions or credit reform funds within the CFO's organization.

C. The Budget Center will:

1. Compile and coordinate all auction operating and credit reform budget requests that are submitted to OMD as well as develop and execute the apportionment requests for auction and credit reform operating funds.
2. Evaluate on an annual basis, the general allocation splits between auction and appropriations, and revise as appropriate.
3. Issue all auction and credit reform allocations to the fund managers or CAM.
4. Verify and record the fiscal year auction and credit reform budget.
5. Coordinate all reprogramming requests.
6. Enter the auction and credit reform's operating budget in the FCC financial system and update the plan throughout the fiscal year.
7. Be responsible for reviewing and approving all auction fund and credit reform requests on behalf of the Bureau's and Office's for the adequacy of the justification and consistency with the original allocation provided.

8. Monitor the execution of Commission-wide auction expenses by tracking all auction related obligations to ensure accuracy in the Auction Expenditure Report annually submitted to Congress as required by statute.
- D. The Financial Systems Operation Group (FSOG) will:
1. Coordinate the flow of documents between the fund managers or CAM to ensure obligations are recorded in the appropriate financial management system.
 2. Assist with recording all auction and credit reform obligations in the Commission's financial system, including space rent, travel, training, credit card purchases, training, and payment of telephone bills.
 3. Issue reports concerning the Commission's use of the auction and credit reform funds and the availability of those funds.
- E. The Wireless Telecommunications Bureau (WTB) will:
1. Be responsible for implementing the competitive bidding authority and incentive auctions authority for spectrum auctions.
- F. The Media Bureau (MB) and the Office of Engineering and Technology (OET) will:
1. Be responsible for implementing the evaluation of the broadcaster television spectrum and making any reassignments or reallocations.
- G. The Information Technology Center (ITC) will:
1. Serve as the management contact for all requests for auction and credit reform funds that will be used for information technology (IT) services or equipment to support the auction program.
- H. The Administrative Operations (AO) Group will:
1. Oversee many of the non-IT-related costs needed to support the auction and credit reform program, such as rent, utilities, security services, housekeeping staff, copier services, and the purchase of goods and services.
- I. The Enterprise Acquisitions Center (EAC) will:
1. Oversee the acquisition of most auction-related goods and services, plus items related to the credit reform use by the Commission.
 2. Retain the contract, and contract solicitations (RFPs) reflecting the use of auction and credit reform proceeds.
 3. Record obligations in the Commission's financial system.

J. Contracting Officers (COs) will:

1. Plan and negotiate contracts on the behalf of the FCC with providers of goods and services.
2. Ensure that the contractual requirements are met in a manner that is most beneficial to the government in terms of price and other relevant factors.

K. Contracting Officer Representatives (CORs) will:

1. Establish the requirements for the goods and services to be acquired as well as managing the contract.
2. Assist the Fund Manger or CAM in the documentation of the funding justification and annual cost estimate of their responsible contracts.

L. Fund Managers or CAMs will:

1. Initiate the approval process by requesting Auction Cost Recovery Funds or Credit Reform Funds for a specific Bureau /Office.

M. The Inspector General will:

1. Conduct, supervise and coordinate audits, inspections and investigations.
2. Keep the Chairman and Congress fully informed concerning any fraud and other serious problems, abuse, and deficiencies related to the auctions and credit reform programs.

8. OFFICE OF MANAGEMENT & BUDGET (OMB) AUTHORIZATION TO USE FUNDS:

A. OMB Current Year Operating Budget Request. OMD shall identify and submit the auction and credit reform operating budgets and apportionment requests (SF-132) to the OMB for funding all auction operating requirements for each upcoming fiscal year beginning on October 1. The apportionment requests for both auctions and credit reform funding shall be made in accordance with OMB requirements. The budget apportionment request from the Commission to OMB shall be developed using data from fund managers and CAMs, including information from the National Finance Center (NFC) payroll system, and the Commission's financial system.

B. Transfer of Funds Following Apportionment. The CFO, in conjunction with the Budget Center, shall request through the Financial Operations Groups that auction receipts deposited into the Treasury be transferred to the Commission's Operating Account for Auctions on a quarterly basis consistent with requirements.

After the specified auction receipts have been transferred by the Department of Treasury to the current year Auctions Operating Budget (Fund X54), the Budget Center shall establish operating budget allocations for each Fund Manager or CAM. Fund Managers and CAMs cannot exceed the allowances made under any circumstances without CFO approval. Authorized obligations shall be charged directly against Fund X54 and Credit Reform (Fund CR2), in the financial system fund account established to fund auction and credit reform program costs. Operating requirements that serve multiple purposes must be funded from appropriated, auctions funds, and/or credit reform funds. These “split funded” items and the distribution of cost must be fully justified by the bureau, office and CAM with documented rationale for the percentage split. If there is any uncertainty or question about the amount of auction or credit reform funds to use on any obligation the CFO should be consulted.

- C. Carryover Authority. Under Section 309(j), as amended, unobligated auction receipts retained in the Commission’s appropriation accounts at the end of a current fiscal year may be forwarded into the next fiscal year through the transfer of current year balances into the next year or “no-year” accounts. Such funds may be used to prevent interruption of auction support activities during OMB’s review of the Commission’s requested auction operating plan for the new fiscal year. Operating funds must be apportioned by OMB and moved by Treasury to the proper account prior to any obligation of funds. This practice of ensuring sufficient funds are available over the transition of the fiscal year is still required for the credit reform administration.

Note: Beginning with FY 2014, OMB approved the auctions program account (Fund X54) as no-year funds. As result, unobligated funds at the end of the fiscal year in Fund X54 remains in the account until expended. There is no longer the need to carryover the unobligated funds to subsequent fiscal years.

- D. OMB Budget Year Estimates. The FCC’s annual appropriation based budget request is due to OMB in September each year. OMD’s proficiency in compiling estimates of Commission appropriation needs are highly dependent on the anticipated needs for auction and credit reform funding. These estimates are dependent on the level of information and cooperation provided by the bureaus, offices and CAMs that use auction and credit reform funds. The process involves a review of current year expenditures, annualization and adjustments for inflation, and then consideration of new initiatives within available funding. OMD then provides summaries and the adequately justified request from the bureaus and offices to the Chairman for approval. Once approved, the budget package is provided to OMB. OMB then evaluates this request and determines what amount should be included in the President’s Budget that is then transmitted to Congress. After the FCC’s appropriation amount is approved by Congress and signed by the President, an apportionment is submitted by the Commission to OMB and approved by OMB.

9. CATEGORIES OF AUCTION COST RECOVERY AND CREDIT REFORM FUNDS

USE: Auction and credit reform operating expenditures shall be divided into two main categories of auction and credit reform-related expenses: (1) Direct Program Costs; and (2) Commission-wide Program Support Costs.

A. Direct Program Expenditures. Direct auction program expenses are those that directly support the auction and credit reform program. These auction-related costs tend to be items that are directly controlled by WTB and MB, although certain Investment Technology (IT) and Financial Operations (FO) expenses have been considered direct costs in the past. The credit reform-related costs tend to be items that are directly controlled by the WTB, Office of General Counsel (OGC) or FO. To qualify, an expense must be directly and solely related to the policy development, implementation and execution of the auction program or credit reform, such as:

1. Employee salaries and benefits;
2. Computer and telecommunications equipment, software, and services;
3. The conduct and maintenance of all technical auction operations, including the planning, installation, operation, and maintenance of related information technology systems and telecommunications equipment hardware and software;
4. All network automation requirements necessary to link the Commission with auction participants and others involved with the collection and management of auction funds;
5. Contracts providing support to the auction and credit reform programs;
6. Travel necessary to conduct audits to ensure the integrity of one or more auctions and credit reform;
7. Travel and seminar costs to educate the public and government (both domestic and foreign) regarding auctions;
8. Training and travel that is necessary to educate FCC staff regarding collections, auction theory and other issues associated with auctions;
9. Equipment and travel necessary to identify potential spectrum to auction;
10. Office supplies and software, to address on-going needs of personnel assigned to support auction activities prior to, during, and after each auction and credit reform;
11. Investigation to ensure the integrity of the auction programs, including non-federal legal support to resolve bankruptcy litigation and matters related to installment loans;
12. Other costs directly required to support the auctions program;
13. Legal costs through OGC associated with the auction and credit reform programs; and
14. FO contracts associated with the auction and credit reform programs.

- B. Commission-wide Program Support Costs. This category is made up of indirect (overhead) costs that support all Commission activities, such as:
1. Overhead costs that support the day-to-day operation of the Commission, like human resources, information systems technology (software, hardware, support contracts, telecommunications), financial operations, administrative services (shared facilities rent, guard services, contract services, utilities), general counsel, inspector general, Office of Secretary, media relations, strategic planning and policy, and performance evaluation and record management; and
 2. Other functions that support management of the Commission as whole.
10. INDIRECT COST ALLOCATION METHODS: Indirect costs shall be allocated using one of the following methods for auction cost recovery, as appropriate:
- A. Full Time Employee (FTE) Employee Rate (Generally Allocated). This rate is derived from the percentage of actual hours worked, including a proportionate share of the employee's indirect hours (leave hours) that were used in support of the auction and credit reform programs as recorded in the Commission's financial system. The FTE Employee rate will normally be applied to costs for items that benefit Commission-wide allocation to the Auction Cost Recovery. Cost items that are allocated by the FTE rate include: Commission-wide information systems, guard service, administrative facility services, supplies, furniture, equipment, and human resources training activities. Indirect costs to be allocated to the auction program using this method shall be determined by calculating a ratio based on the proportion of FTEs devoted to supporting the auction's program relative to the total number of FTEs Commission-wide. The Commission has determined from historical data that 14% is an acceptable rate. The Budget Center will review and evaluate this rate on an annual basis and notify bureaus, offices and CAMs if the rate is to be adjusted for any fiscal year. Once the FTE ratio for indirect costs (often referred to as the overhead percentage) has been established for the budget fiscal year, it should not be changed unless a very compelling case can be made, *e.g.*, it is determined that the allocation formula was erroneous.
- B. Square Footage Percentage Split. This percentage split is derived from calculating the square footage used by either appropriation or auctions funded activities and dividing it by the Commission's total square footage. Cost items that are typically allocated by the square footage percentage split include rent and utilities for the Gettysburg office. Under this calculation, the auctions fund percentage split is equal to auctions funded activities divided by the total square footage. When added, the appropriations and auctions percentages should equal 100%. The square footage percentage split will be developed by OMD-Administration Operations, with approval of the Budget Center.

activities and dividing it by the Commission's total square footage. Cost items that are typically allocated by the square footage percentage split include rent and utilities for the Gettysburg office. Under this calculation, the auctions fund percentage split is equal to auctions funded activities divided by the total square footage. When added, the appropriations and auctions percentages should equal 100%. The square footage percentage split will be developed by OMD-Administration Operations, with approval of the Budget Center.

- C. Special Allocation Rate. This represents an allocation method that has been proven more appropriate for a particular cost than the aforementioned methods. When it is determined that another method would be better suited in allocating the cost to the Auction Cost Recovery Fund or Credit Reform Fund, the COR, Fund Manager, or CAM will be responsible for obtaining the approval of the Budget Center and the CFO.
10. ETHICAL CONDUCT: To ensure that every citizen can have complete confidence in the integrity of the Commission, each Commission employee shall adhere to the Commission's Code of Conduct ("Code of Conduct") set forth in the Policy for Detecting and Deterring Fraud and Promoting Ethical Conduct within the Federal Communications Commission ("Anti-Fraud Directive") with regard to apportioning and obligating spectrum auction funds for the Commission's auction and credit reform program expenses as contained in this Directive. The Code of Conduct is designed to deter wrongdoing and promote: (1) full, fair, accurate, timely, and understandable disclosure in reports and documents; (2) compliance with applicable governmental laws, rules, and regulations; and (3) the prompt internal reporting of violations of the Code of Conduct to an appropriate person or persons identified herein. All employees shall report instances of suspected irregularities to the Commission's Office of Inspector General in accordance with the Commission's Anti-Fraud Directive.
11. EFFECTIVE DATE AND IMPLEMENTATION: This directive is effective immediately and shall be implemented promptly upon distribution.


Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Audit Follow-Up	
	Directive Number: FCCINST 1013.3	Effective Date: October, 2014

1. Purpose and Applicability. This directive establishes audit follow-up policies and procedures. These policies and procedures are established pursuant to Office of Management and Budget (“OMB”) Circular A-50, “Audit Follow-up,” dated September 29, 1982, and the Inspector General Act, as amended, and are designed to enhance the benefits that accrue to the Commission from audits of its operations, programs, systems, functions, activities and controls. They apply to audit reports issued by, or under the sponsorship of, the Office of Inspector General (“OIG”) or by the U.S. Government Accountability Office (“GAO”) whenever follow-up is necessary.
2. Cancellation. This directive supersedes FCCINST 1013.2 dated November 7, 2012.
3. Definitions.
 - a. Draft Audit Report. An audit report that has been released to the auditee and that has been submitted to management for comment. For purposes of this guidance, the term audit report encompasses audits, inspections, or evaluations conducted by the OIG or GAO.
 - b. Final Audit Report. An audit report that has been made available to the public or otherwise determined to be final by the auditor. For purposes of this guidance, the term audit report encompasses audits, inspections, or evaluations conducted by the OIG or GAO.
 - c. Responses to Audit Reports. Written comments by appropriate Bureau or Office chief(s) indicating agreement or disagreement on recommendations in draft or final audit reports. Comments indicating agreement shall include planned corrective actions to the extent possible within the time frame for responding, and, where appropriate, dates for achieving actions. Comments indicating disagreement shall fully explain the reasons for disagreement. Efforts to resolve potential non-concurrences on GAO and OIG audit recommendations shall be first made at the lowest possible management level before escalating.
 - d. Fund Administrator. The administrator of the Universal Service Fund (“USF”) or the Telecommunications Relay Service (“TRS”) fund.
 - e. Audit Follow-up Official. The Managing Director or the Managing Director’s designee shall serve as the Audit Follow-up Official.
 - f. Resolution.

- (1) The point at which the OIG and the appropriate Bureau or Office Chief(s) agree on action to be taken on an audit report's findings and recommendations, or, if no agreement can be reached, the point at which the matter is determined to be resolved by the Audit Follow-up Official. An audit report may be considered resolved despite the right of persons outside the Commission to negotiate, appeal, or litigate. Resolution of a report with respect to parties outside the Government does not preclude further consideration of issues in the report by Commission management.
 - (2) For pre-award contract audits, the point at which agreement is reached, a contract price negotiated, or a proposed award canceled, whichever occurs first.
 - (3) For GAO reports with recommendations to the Chairman, the point at which the GAO and the appropriate Bureau or Office Chief(s) agree on action to be taken on an audit report's findings and recommendations, or, if no agreement can be reached, the point at which the matter is determined to be resolved by the Audit Follow-up Official. The resolution process with GAO will be informed by the Chairman's written statement on the recommendations submitted to Congressional committees within 60 days of the issuance of the GAO report, as required by 31 U.S.C. § 720.
- g. Corrective Action - Measures taken to implement resolved audit findings and recommendations.
 - h. Corrective Action Plan - A written plan prepared by management to describe specific steps and target dates for implementing corrective action.
 - i. Disallowed Costs - Incurred costs that have been questioned by the audit organization and that the contracting officer or other appropriate Commission official has agreed should not be charged.
4. Policies.
- a. Audit follow-up is an integral part of good management, and is a shared responsibility of Commission management officials and auditors. Corrective action on resolved audit findings and recommendations is essential to improving the effectiveness and efficiency of government operations.
 - b. Management has an obligation to address audit results. Management will make every reasonable effort to respond to OIG draft audit reports. If management is unable to respond to an OIG draft audit report, (*e.g.*, due to time constraints or to the need for further investigation of report findings), management must respond to the final audit report.
 - c. Written responses to draft audit reports will be due within 30 days of the issuance of the Draft Audit Report. Management may, upon request, obtain a reasonable extension of the due date for good cause shown. Consistent with GAO standards for audits, auditors should provide management an opportunity to respond to the Draft Audit Report. *See* Government Auditing Standards (GAO-12-331G), December 2011 Revision, sections 7.32 – 7.38. The response may be written or oral, but written comments are preferred.
 - d. Except otherwise indicated herein, written responses to audit recommendations will be prepared by the Bureau or Office chief(s) responsible for the audited activity and will be transmitted to the

Inspector General or the GAO via the Audit Follow-up Official. If management's response to a recommendation contemplates any corrective action, a Corrective Action Plan will be included in the response to the extent possible. In such cases, if a Corrective Action Plan is not included in the response to the draft report, the Bureau or Office responsible for the audited activity will prepare a Corrective Action Plan within 30 days of the issuance of the final report and transmit the Corrective Action Plan to the Audit Follow-Up Official, who will transmit the Corrective Action Plan to the OIG or GAO.

- (1) For audits of USF or TRS beneficiaries or contributors, and for audits of the USF and TRS fund administrators, the actual Fund Administrator shall respond to Draft Audit Reports under the guidance of the Office of Managing Director ("OMD"), as determined necessary by OMD. The Fund Administrator shall state whether it agrees with the factual findings in its response to the Draft Audit Report, as well as the recommendations (see paragraph 6, *infra*). In addition, the Fund Administrator shall start to implement any recommendations that it has agreed with, *e.g.*, recovery of funds, within 30 days of issuance of the final audit report.
 - (2) The OMD will, as appropriate, ensure that the Fund Administrator seeks recovery of funds as recommended in Final Audit Reports if the Fund Administrator has agreed that the facts are correct.
 - (3) The Wireline Competition Bureau ("WCB") will handle all appeals filed by USF beneficiaries or contributors of any contested audit recommendations (*e.g.*, an audit recommendation to recover funds). The Consumer and Governmental Affairs Bureau ("CGB") will handle all appeals related to the TRS fund.
- e. When applicable, the resolution process begins once the OIG receives a Bureau's or Office's response to a Draft Audit Report or upon issuance of the Final Audit Report if management does not respond to the Draft Audit Report. The OIG and the affected Bureau(s) or Office(s) will make every effort to reach resolution on audit recommendations prior to issuance of the final audit report. If written responses to draft audit reports are not provided prior to issuance of the final audit report, those responses and resolution must be completed within six months from the date the final audit report is issued or, under special mitigating circumstances, within a reasonable period of time thereafter. As mentioned above, whenever corrective action is contemplated, a Corrective Action Plan will need to be provided to the Audit Follow-Up Official as part of the recommendation resolution process if one has not been provided already at this point in the process.
- f. The OIG will provide a copy of the final audit report to the affected Bureau(s) or Office(s) and the Audit Follow-up Official. If resolution has not already begun or was not reached prior to issuance of a final report, it shall commence immediately and shall be completed within six months from the date the final report is issued, or, under special mitigating circumstances, within a reasonable period thereafter. Resolution shall include a proposed corrective action plan where appropriate.
- g. Responsible officials must keep the Audit Follow-up Official, or his or her designee, notified of the progress made in meeting each planned date contained in a Corrective Action Plan.

Additionally, responsible officials must provide documentary support to the Audit Follow-up Official, or his or her designee, upon completion of corrective action. The Audit Follow-up Official will transmit the audit resolution information to the OIG and will track whether OIG concurs that a recommendation is closed or needs additional information, etc.

- h. Records will be maintained of the status of audit reports or recommendations throughout the entire process of resolution and corrective action.
- i. Claims attributable to audit disallowances will be brought under accounting and collection controls.
- j. Resolution of findings and recommendations must be consistent with laws/regulations/policies, where applicable.
- k. Semi-annual reports concerning the status of audit reports with disallowed costs, audit reports with recommendations that funds be put to better use, and audit reports with management decisions where final action is still incomplete after one year will be developed by the Audit-Follow Up Official and furnished by the Chairman to the Congress in accordance with the requirements of the Inspector General Act.
- l. Performance appraisals of appropriate officials will reflect their effectiveness in resolving findings and recommendations and implementing necessary corrective actions.

5. Responsibilities.

- a. Bureau/Office Chiefs. Chiefs of Bureaus/Offices are responsible for:

- (1) Reviewing and carefully considering audit reports, or parts thereof, concerning their respective organizations, activities, functions, and programs.
- (2) Preparing or endorsing responses to audit reports and ensuring their timely submission to the OIG or the GAO via the Audit Follow-up Official.
- (3) Informing the Audit Follow-up Official, or his or her designee, of significant disagreements with the OIG or the GAO which prevent resolution and completion of final action on audit recommendations.
- (4) Promptly preparing and implementing written Corrective Actions Plans, as appropriate.
- (5) Directing and monitoring the implementation of promised corrective actions to increase assurance that they are implemented and within applicable specified time limits.
- (6) Maintaining records of the status of corrective action being planned or taken to close audit recommendations, for which the Bureau or Office is responsible, throughout the resolution and corrective action processes and furnishing documentary support to the Audit Follow-up Official

upon completion of corrective action. For audits of USF beneficiaries and contributors and TRS fund beneficiaries and contributors, the Chief Financial Officer will be the party responsible for record maintenance under this subparagraph.

(7) Furnishing information required by the Audit Follow-up Official for the semi-annual report to the Chairman and the Congress.

- b. Audit Follow-up Official. The Managing Director or the Managing Director's designee shall serve as the Audit Follow-up Official. The Audit Follow-up Official has responsibility for ensuring that:

(1) Systems of audit follow-up, resolution, and corrective action are documented and in place.

(2) Timely responses are made to all audit reports.

(3) Disagreements are resolved.

(4) Corrective actions are actually taken.

(5) Semi-annual reports are sent to the Chairman, as provided for in paragraph 10a(1) below.

(6) The USF Administrator and TRS Fund Administrator follow up on audit reports, including those pertaining to USF beneficiaries and contributors.

(7) The USF Administrator and TRS Fund Administrator initiate timely recovery actions against appropriate parties in instances where audits recommend recovery of funds.

- c. Associate Managing Director – Financial Operations (AMD-FO) (also known as “Chief Financial Officer” or “CFO”). Under the Chairman's operational guidance, the AMD-FO administers the internal audit function. In this capacity, he or she is responsible for:

(1) Ensuring that the OIG or the GAO obtain timely responses to their audit recommendations.

(2) Reviewing on behalf of the Audit Follow-up Official responses to audit report recommendations prior to submission to the OIG or the GAO to ensure that the responses conform to the guidelines set forth in paragraph 6 of this directive.

(3) Ensuring that the audited entity develops Corrective Action Plans within 30 days of the issuance of the Final Audit Report for any recommendations in an OIG or GAO audit report for which corrective action is contemplated,

(4) Tracking the status of agency responses to OIG and GAO audit recommendations, and keeping the Audit Follow-up Official informed of the status.

(5) Tracking the status of the USF Administrator's responses to audit reports of USF beneficiaries and contributors and tracking the status of the TRS Fund Administrator's responses to audit reports of TRS beneficiaries and contributors.

(6) Proposing to the Audit Follow-up Official solutions to significant disagreements between the OIG and audit report respondents which may develop (1) prior to the issuance of an OIG Final Audit Report and result in a non-concurrence from the audit respondents to a finding or recommendation or (2) after issuance of an OIG Final Audit Report and prevent resolution and completion of final action on audit recommendations.

(7) Performing follow-up reviews to evaluate the status of the implementation of corrective actions on audit recommendations and communicating with OIG or GAO the necessary information to demonstrate FCC implementation of corrective actions so as to obtain OIG and GAO concurrence on the closure of an audit recommendation for tracking and reporting purposes.

6. Responses to Draft and Final Audit Reports.

a. General.

(1) OIG draft audit reports submitted to management for comment will state the date that a response is desired. Management should provide timely comments to OIG draft audit reports. If necessary, management may request an extension of the due date from the OIG. If the OIG and management are unable to agree on an extension, the OIG may issue the final report without a management response. If a final audit report is issued without a management response, the Audit Follow-up Official will ensure that management submits a corrective action plan for any recommendations in the final report for which corrective action is contemplated and that resolution is completed within six months of issuance of the final report. Corrective action will proceed as quickly as possible.

(2) In certain instances, management may undertake or plan to undertake studies of activities audited that will extend beyond the due date of the Bureau's or Office's responses. When this occurs, comments will not be delayed but will state the action initiated or planned.

b. Contents.

(1) Comments on audit reports will be factual, responsive, and directed to any recommendations. For each recommendation, management should state specifically whether the responding official agrees, partially agrees, or does not agree.

(2) For each time the respondent agrees with an audit recommendation, the respondent should explain the specific action that will be taken, initiated, or planned when appropriate. For example, if the action involves the issuance of new or revised procedures, copies of such procedures or pertinent extracts should be provided. If further action is required, a target completion date should be furnished. When the action is completed, the responding official shall promptly advise the AMD-FO in appropriate detail so the AMD-FO may communicate the implemented corrective action to the OIG or GAO.

(3) Each partial agreement or disagreement will be fully explained.

(4) If a report sets forth questioned costs which the contracting officer or other appropriate Commission official agrees should not be charged, the response should provide the amounts of

payment demanded, the amounts recovered by collection and/or offset, or, in case of a decision not to seek recovery, the basis for the decision.

7. Supplemental Provisions for GAO Reports. The following additional provisions apply to the processing of GAO audit reports.
 - a. Coordinating Responsibilities. The AMD-FO has been delegated responsibility in support of the Office of the Chairman and the Managing Director for coordinating comments on draft GAO reports or responses to final GAO audit reports with recommendations to the Chairman. In this capacity, the AMD-FO will:
 - (1) Distribute GAO audit reports to organizational elements that are affected by or are likely to be interested in such reports.
 - (2) Designate the action office with primary responsibility for preparing a reply to a report.
 - (3) Establish due dates regarding the submission of involved organizational elements' written comments to the action office, where applicable, and the action office's preparation of the reply.
 - b. Draft Reports. Normally, GAO will furnish the Commission a draft report setting forth findings and recommendations which have been developed during its examination and which have been discussed during an exit conference. The draft is furnished to permit the Commission to express its written views on any part of the report as a basis for GAO revision, clarification, or citation respecting the final report. Replies to draft reports will be prepared and processed in accordance with the following procedures:
 - (1) General. Commission policy is to respond to any GAO draft report received by the date requested by the GAO or by an extended due date authorized by the GAO. Pursuant to 31 U.S.C. § 718(b), the statutory period for providing comments on draft GAO reports is generally no more than 30 days, but the GAO usually requests comments within 7 to 14 days after the Commission receives the draft report. The designated action office should complete the reply by the due date established by the AMD-FO. If an extension of time is needed, the action office should notify the AMD-FO as soon as it knows an extension will be necessary. In turn, the AMD-FO will request an extension of time from GAO and will, in consonance with the additional time authorized by GAO, promptly establish revised due dates for submission of comments by organizational elements and the action office's reply, and appropriately communicate such dates.
 - (2) Preparation of Reply. The lead Bureau or Office responsible for responding to GAO throughout the audit will take the lead on drafting the reply and ensure that GAO's timeline for delivery is met. The lead Bureau or Office shall ensure that the reply is responsive, clear, and consistent with Commission policies, regulations, and procedures. When the report involves multiple Bureaus or Offices, each organizational element affected by the report will submit to the lead Bureau or Office the appropriate written comments in a timely manner for use in preparation of a coordinated reply. Furthermore, the lead Bureau or Office should coordinate with the Office of General Counsel and Office of Legislative Affairs to obtain their review (as necessary). Finally, the lead Bureau or Office will ensure that the Office of the Chairman has an opportunity to review the reply before it is finalized for signature. If the reply is in the form of a

letter, the lead Bureau or Office will prepare the letter for the signature of the Chief of their Bureau or Office. Following final approval and signature (as necessary), the lead Bureau or Office will transmit the reply to the AMD-FO, who will ensure timely delivery to GAO.

- c. Final Reports. Responses to final reports will be prepared and processed, giving due consideration to the general criteria contained in paragraph 6b above and the specific requirements and instructions set forth in paragraph 7d below.
- d. Statements on Final Reports.

(1) Statement to Congressional Committees. In accordance with 31 U.S.C. § 720(b), when a GAO report contains recommendations to the head of a Federal agency, the agency shall:

(a) Submit a written statement to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform no later than 60 days after the date of such report (“60 day letter”). This statement will report the action taken or to be taken by the agency with respect to the recommendation to the agency head.

(b) Submit a written statement to the Committees on Appropriations of the Senate and the House of Representatives in connection with the first request for appropriations by the FCC submitted to Congress more than 60 days after the date of the GAO report. The statement will report the action taken or to be taken by the agency with respect to the recommendations to the agency head. The Commission may satisfy this requirement by including in its annual budget submission to the Congress copies of statements submitted in accordance with paragraph 7d(1)(a) above.

(2) Statements to OMB and GAO.

(a) OMB Circular A-50, Revised, September 29, 1982, requires that OMB and GAO each be furnished two copies of the statements provided the Congressional committees in accordance with 31 U.S.C. § 720(b). These copies should be submitted at the time of submission of the statements to the Congressional committees.

(3) Preparation of Replies.

(a) Statements or replies to Congress on final GAO reports should identify the applicable GAO report by number and date (*e.g.*, GAO-14-236, dated February 26, 2014).

(b) The same lead Bureau or Office that developed the original response to the draft report should develop a proposed coordinated reply for the 60 day letter to the House and Senate Oversight Committees using procedures similar to those set forth in paragraphs 7 b above, except that the reply will be prepared for signature by the Chairman.

8. Applicability to Pre-award Contract Audits. In general, audit reports involving recommendations on contractor estimates of future costs are subject to the provisions of this directive. Because such reports are usually resolved by negotiation of a contract price, however, they are not subject to either the 6-month resolution or the semi-annual reporting provisions cited elsewhere in this directive. Also, insofar as the previously and subsequently referenced requirement for maintaining records of the status of audit reports or recommendations through the entire process of resolution and corrective action is concerned, it will be met relative to pre-award contract audits by the maintenance of appropriate records as part of the official procurement files.

9. Accounting and Collection Controls. The Chief Financial Officer, will establish and maintain collection and accounting controls over amounts due the Government as a result of disallowed costs, and will ensure that:


- a. Amounts due the Government as a result of audit disallowances are promptly recorded as accounts receivable upon completion of the acts entitling the Commission to collect them. Within 30 days of a determination by the contracting officer or other appropriate Commission official that incurred costs questioned by audit are unallowable, the amounts of the disallowances will be recorded as accounts receivable.
- b. Prompt and appropriate action is taken to collect amounts of audit disallowances due the Government. Amounts of audit disallowances (only disallowed costs, not relevant interest charges, if applicable) recovered, whether by collection or offset, will be credited to the appropriations charged with pertinent incurred costs and applied as decreases to respective previously established accounts receivable.
- c. Interest on audit-related debts is accrued beginning no later than 30 days from the date a debtor is notified of his or her indebtedness and the accrual is continued during the period, if any, that the Government's claim may be under appeal. Interest is to be accrued at applicable interest rates prescribed in the Treasury Financial Manual. Amounts collected for accrued interest are to be deposited into the U.S. Treasury as miscellaneous receipts unless there is specific statutory authority for some other disposition.

10. Records Maintenance and Semi-Annual Reports.

- a. Bureau/Offices. Bureaus/Offices responsible for implementing open recommendations will maintain records showing the status of corrective action being planned or taken to close audit recommendations, for which the Bureau or Office is responsible, throughout the entire process of resolution and corrective action. In addition, if the recommendation relates to an information technology system, the Bureaus/Offices should coordinate with the FCC's Chief Information Officer to ensure that all corrective action is properly documented for audit follow up purposes. These records should be used to furnish the Audit Follow-up Official and AMD-FO with documentary support for corrective action taken in response to each OIG or GAO recommendation, and to provide the information required for the semi-annual report described in subparagraph 1 below.

(1) Audit Follow-up Official. The Audit Follow-up Official will furnish the Chainnan semi-annual reports with certain information concerning audit reports with disallowed costs, audit reports with recommendations that funds be put to better use, and audit reports with management decisions where final action is still incomplete after one year (as specified in the Inspector General Act, as amended, 5 USC, Appendix 3, Section 5). The Audit Follow-up Official will ensure that the USF Administrator follows up on USF-related audit reports, including audit reports of USF beneficiaries and contributors. For audits of USF beneficiaries and contributors, the Chief Financial Officer will coordinate with the USF administrator to obtain the necessary information for this section. In addition, the Audit Follow-up Official will ensure that the TRS Fund Administrator follows up on TRS Fund-related audit reports, including audit reports of TRS fund beneficiaries and contributors. For audits of TRS fund beneficiaries and contributors, the Chief Financial Officer will coordinate with the TRS administrator to obtain the necessary information for this section.

(2) Reports will be prepared as of every March 31st and September 30th and will be submitted to the Chainnan by the 30th workday following the end of the semi-annual reporting period.

A handwritten signature in black ink, appearing to read 'Jon Wilkins', with a long horizontal flourish extending to the right.

Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Administrative Control of Funds	
	Directive Number: FCCINST 1036.3	Effective Date: July 2015

1. **PURPOSE:** This directive sets forth the Federal Communication Commission's (Commission's) policies, procedures and responsibilities relating to administrative control of funds and budget execution. The directive also explains basic fund control principles and concepts. In particular, the directive:
 - A. Prescribes a system for positive administrative control of funds designed to restrict obligations and expenditures (disbursements) to the amount available in each appropriation account or fund account.
 - B. Restricts both obligations and expenditures from each appropriation or fund account to the lower of the amount of apportionments made by the Office of Management and Budget (OMB) or the amount available for obligation and/or expenditure in the appropriation or fund account.
 - C. Enables the Chairman of the Commission to identify the person responsible for any obligation or expenditure exceeding the amount available in the appropriation or fund account, the OMB apportionment or reapportionment, the allowances made by the Commission, any statutory limitations, and any other administrative subdivision of funds made by the agency.
 - D. Provides procedures for addressing violations of the Antideficiency Act as well as violations of other administrative subdivision of funds that are not violations of the Antideficiency Act *per se*.
 - E. Enables the Chief Financial Officer (CFO) to determine responsibility for Antideficiency Act violations and to take necessary corrective action.
 - F. Ensures that funds shall be expended solely for the purposes for which they were appropriated, except as otherwise provided by law.
 - G. Provides that obligations or expenditures shall not be authorized or incurred in excess of available funds or in excess of any legal or administrative limitations including but not limited to apportionments and reapportionments;
 - H. Ensures that only valid obligations shall be recorded in the accounting records, and all obligations incurred shall be recorded accurately and promptly; and
 - I. Provides that outstanding obligations shall be validated annually.

2. SCOPE: This Directive applies to all Bureaus and Offices of the Commission. Any exceptions to this Directive must first be approved by the CFO, Managing Director, Chairman and then by OMB.
3. AUTHORITY:
- A. The Antideficiency Act of 1906, as amended (31 U.S.C. §§ 1341-1342, 1349-1351, and 1511-1519);¹
 - B. Budget and Accounting Act of 1921, as amended (31 U.S.C. §§ 1101, 1104-1108, 3324);
 - C. Budget and Accounting Procedures Act of 1950 (31 U.S.C. §§ 1112, 1531, 3511-3512, 3524);
 - D. Supplemental Appropriations Act of 1950 (31 U.S.C. §§ 1501-1502);
 - E. National Defense Authorization Act of 1990 (31 U.S.C. § 1552);
 - F. Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. §§ 681-688);
 - G. Federal Credit Reform Act of 1990, as amended (2 U.S.C. § 661); and
 - H. Instructions, procedures, guidelines, circulars, bulletins, memoranda, and definitions issued by the Office of Management and Budget (OMB), the United States Government Accountability Office (GAO), and the Secretary of the Treasury for agencies to follow in properly controlling their budget authority, including:
 - (1) OMB Circular No. A-11, "Preparation, Submission and Execution of the Budget" Revised June 2015;
 - (2) The Treasury Financial Manual;
 - (3) GAO, A Glossary of Terms Used in the Federal Budget Process, GAO-05-734SP (September 2005); and
 - (4) FCC Policies and Procedures Manual, Chapter 2.
4. POLICY: It is the policy of the Chairman that standard practices be established and followed both at the Commission and reporting components that are, or may become subject to, the Antideficiency Act to ensure compliance with the Antideficiency Act, as set forth in this

¹ In 2005, Congress granted the Universal Service Fund (USF) a one year exemption from the Antideficiency Act for calendar year 2005. Universal Service Antideficiency Temporary Suspension Act, Pub. L. 108-494, title III, Dec. 23, 2004, 118 Stat. 3997. Congress has extended this temporary suspension in one and two year increments. Consolidated and Further Continuing Appropriations Act, 2015, Pub. L. 113-235, 128 Stat. 2130 (2014) at § 501 ("Section 302 of the Universal Service Antideficiency Temporary Suspension Act is amended by striking "December 31, 2015," each place it appears and inserting "December 31, 2016.").

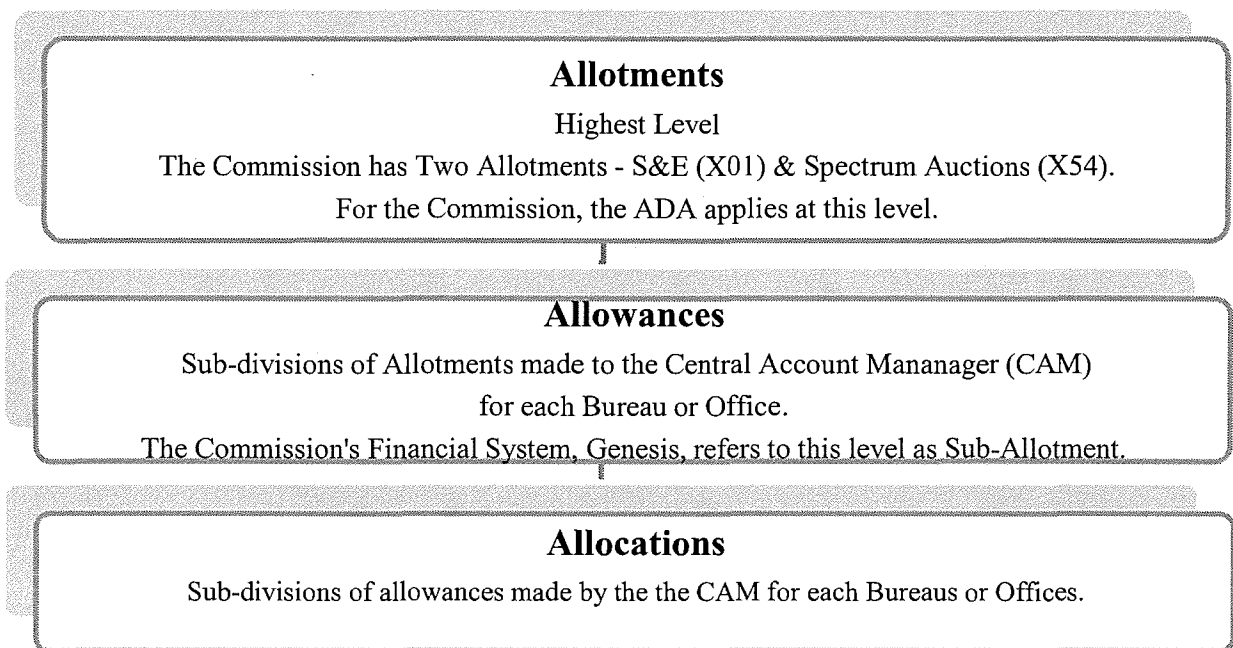
directive. Program and budget officials shall perform administrative funds control by planning, programming, and utilizing integrated budget and accounting systems to preclude Antideficiency Act violations. The CFO shall investigate and determine responsibility for Antideficiency Act violations. If deemed appropriate, an office may utilize local systems to complement and enhance the control, recording, and reporting of accounting and budgetary activities and the status of the budget.

5. DEFINITIONS/TERMINOLOGY/CONCEPTS: Many of the definitions are taken from the most recent edition of OMB Circular No. A-11. For terms or concepts not found in OMB Circular No. A-11, refer to GAO Glossary of Terms Used in the Federal Budget Process, GAO-05-734SP (September 2005).

- A. Administrative Division or Subdivision of Funds – means apportionment or other distribution of an appropriation or fund made pursuant to the Antideficiency Act. The appropriation may be divided or subdivided administratively within the limits of the apportionment (31 U.S.C. § 1513(d)). The expenditure or obligation of the divided or subdivided appropriation or fund may not exceed the apportionment.
- B. Allotments – are subdivisions of the apportionment that are made by the head of the agency. For the Commission, Allotment is equal to apportionment.
- C. Allowances – are subdivisions of allotments. The Commission uses the term allocations to designate sub-divisions of allowances.
- D. Antideficiency Act – is a statute that prohibits the making or authorizing of an expenditure or creating or authorizing an obligation (i) in advance of an appropriation, (ii) in excess of amounts available in an appropriation or fund accounts unless specifically authorized by law, or (iii) in excess of an apportionment or reapportionment or in excess of other subdivisions made pursuant to 31 U.S.C. §§ 1513-1514, 1517. This statute also prohibits the acceptance of voluntary or personal services unless authorized by law, requires OMB to apportion appropriated funds and other budgetary resources to executive branch agencies, requires the head of each agency to prescribe a system of administrative controls, and specifies penalties for violations of the Antideficiency Act.
- E. Apportionment – is a plan, approved by OMB, to spend resources provided by one of the annual appropriations acts, a supplemental appropriations act, a continuing resolution, or a permanent law (mandatory appropriations). Resources are apportioned by Treasury Account Fund Symbol (TAFS). The apportionment identifies amounts available for obligation and expenditure. It specifies and limits the obligations that may be incurred and expenditures made (or makes other limitations, as appropriate) for specified time periods, programs, activities, projects, objects, or any combination thereof. An apportioned amount may be further subdivided by an agency into allotments, suballotments, and allocations. The Commission uses the following terminology with respect to subdivisions of apportionment:
 - i. The term allotment is used interchangeably with apportionment;
 - ii. The term allowance means a subdivision of allotment/apportionment;
 - iii. The term allocation means a subdivision of an allowance.

- iv. The term “sub-allocation” is not used by the Commission in its funds control policies. The Commission’s financial system, Genesis, however, refers to allowance as a “sub-allotment.”
- F. Budget Authority – means the authority provided by law to incur financial obligations that will result in outlays. The specific forms of budget authority are appropriations, borrowing authority, contract authority, and spending authority from offsetting collections.
- G. Budgetary Resources – means amounts available to incur obligations in a given year. Budgetary resources consist of new budget authority and unobligated balances of budget authority provided in previous years.
- H. Commitment – means an administrative reservation of allotted funds, or of other funds, in anticipation of their obligation. As pre-obligations, commitments are internal actions that are not legally binding. However, for administrative control of fund purposes, commitments are treated as reductions in available budgetary resources. The use of the term “commitment” in the administrative control of funds process is consistent with the U.S. Government Standard General Ledger.
- I. Expenditure – is an outlay or disbursement.
- J. Obligation – means a binding agreement that will result in outlays, immediately or in the future. Budgetary resources must be available before obligations can be incurred legally.
- K. Outlay – means a payment to liquidate an obligation (other than the repayment of debt principal or other disbursements that are "means of financing" transactions). Outlays generally are equal to cash disbursements but also are recorded for cash-equivalent transactions, such as the issuance of debentures to pay insurance claims, and in a few cases are recorded on an accrual basis such as interest on public issues of the public debt. Outlays are the measure of Government spending.
- L. Rescission – means a proposal by the President to reduce budgetary resources (new budget authority or unobligated balances of budget authority) pursuant to the requirements of Title X of the Congressional Budget and Impoundment Control Act of 1974. Resources that are proposed by the President for rescission may be withheld from obligation for 45 calendar days of continuous session of the Congress (excluding an adjournment of more than three days on which either House is not in session) pending congressional action on the proposal. The term is often used more broadly to refer to any legislative action taken by the Congress to reduce budgetary resources, including reductions that were not proposed pursuant to the Impoundment Control Act. Rescissions can either be temporary or permanent.
- M. Sub-allotment – An administrative subdivision of funds. Note: Sub-allotments are not used by the Commission. Instead, the Commission uses the term allowances (see explanation above).

The following diagram shows the different levels of fund control and the terminologies used at the Commission:



6. **RESPONSIBILITIES:** The Chairman has overall responsibility for establishing an effective administrative control of funds process and the CFO is responsible for implementing and maintaining that process. Each Commission allowance holder is responsible for the proper management and control of funds in his or her respective allowance. All Commission employees who are involved in funds control are responsible for adhering to the Commission's policies for the administrative control of funds as described in this directive. It is the responsibility of any employee who has knowledge of circumstances that may lead to or constitute a possible violation of the Antideficiency Act to provide this information to the CFO for consideration and appropriate action in accordance with this directive. Additional positions within the Commission charged with funds control responsibilities are described below.

A. **Chief Financial Officer:**

- (1) Implements a financial system that support Commission administrative control of funds that include recording financial transactions affecting: apportionments; reapportionments; Commission restrictions; spending plans; commitments, obligations, and expenditures; and anticipated, earned, and collected reimbursements;
- (2) Plans and structures new programs or activities to provide for administrative control of funds in accordance with this directive;
- (3) Ensures that reporting entities subject to the Antideficiency Act have sufficient administrative control of funds in place to prevent and detect violations;

- (4) Provides guidance and training on policies and procedures for the administrative control of funds;
- (5) Designates certifying officers for oversight of payment controls and certification of payments processed by the Financial Operations Center;
- (6) Prepares and reconciles financial reports that display cumulative obligations and the remaining unobligated balances by appropriation and cumulative obligations by Bureau and Office and object class;
- (7) Provides reporting on the status of amounts committed, obligated, unobligated, expended or withheld, for management information and decision making; and
- (8) Investigates potential violations of the Antideficiency Act, determines if actual violations have occurred, reports on any violations, and ensures that the Commission takes corrective action on any such violations, as well as violations of other administrative subdivisions of funds that are not violations of the Antideficiency Act, *per se*.

B. Budget Officer:

- (1) Maintains an up-to-date inventory of apportionments, allotments and allowances;
- (2) Processes apportionment, reapportionment, allotment and reprogramming requests;
- (3) Monitors the budget formulation and appropriations process to identify changes to the Commission's budget authority that would warrant changes to apportionments and allowances;
- (4) Develops a spending plan for submission to Congress, when required;
- (5) Issues subdivision of apportioned funds as budget allowances to Bureaus and Offices to support program or administrative operations;
- (6) Processes allowance and allocation adjustment requests;
- (7) Monitors budget execution and advises allowance holders on funding use and needs;
- (8) Reports promptly to the CFO any unanticipated need for funds not budgeted at the beginning of the fiscal year;
- (9) Reports promptly to the CFO any potential violations of the Antideficiency Act; and

- (10) Supports the CFO in the investigation, report, and follow-up actions of possible Antideficiency Act violations and violations of Commission limitations that are not violations of the Antideficiency Act.

C. Allotment Holder – Chairman’s Chief of Staff:

- (1) Bears overall responsibility for funds allotted to them;
- (2) Reports promptly to the CFO any potential violations of the Antideficiency Act; and
- (3) Supports the CFO in the review, resolution and reporting of possible Antideficiency Act violations regarding funds allotted to them. [Note: At the Commission, there is only one allotment holder].

D. Allowance Holders – Central Account Managers – One for each Bureau or Office:

- (1) Bear overall responsibility for the funds allocated to them;
- (2) Manage and control commitments, obligations, and expenditures in accordance with the limitations of their allowances;
- (3) Report promptly to the CFO any potential violations of the Antideficiency Act; and
- (4) Support the CFO and allotment holder in the review, resolution and reporting of possible Antideficiency Act violations regarding funds allocated to them.

E. Bureau or Office Program and Administrative Staff Processing Requests for Commitments, Obligations, and Payments:

- (1) Identify the source, time period, and use of the budgetary resource associated with the funding action being requested;
- (2) Obtain required reviews and signatures to approve the requested funding action;
- (3) Obtain required verification of the availability of funds prior to making commitments, obligations, or payments;
- (4) Maintain documentation in support of all commitment, obligation, and payment events;
- (5) Validate the system’s processing of requests for commitment, obligations, and payments; and
- (6) Report promptly to the CFO any potential violations of the Antideficiency Act.

F. Office of General Counsel:

Resolve legal questions referred that involve the law of appropriations, such as availability of amounts appropriated with respect to purpose, time or amount; or that arise from financial statutes such as the Antideficiency Act, giving careful consideration to provisions in specific appropriations laws as well as pertinent program authorization language.

7. ACTIONS PROHIBITED:

The Antideficiency Act is codified in 31 U.S.C., Chapters 13 and 15. The act prohibits:

- A. Making or authorizing an expenditure from, or creating or authorizing an obligation under, any appropriation or fund in excess of the amount available in the appropriation or fund unless authorized by law;
- B. Involving the government in any contract or other obligation for the payment of money for any purpose in advance of appropriations made for such purpose, unless the contract or obligation is authorized by law;
- C. Accepting voluntary services that could give rise to claims against the United States Government or employing personal services in excess of that authorized by law, except in the cases of emergency involving the safety of human life or the protection of property;
- D. Making obligations or expenditures in excess of an apportionment, reapportionment, allotment or sub-allotment, or in excess of the amount permitted by agency regulations;

While all actions should be reviewed for potential Antideficiency Act concerns, the following are often particularly problematic:

Multi-year contractual commitments – contracts for the purchase of supplies or services for more than one year (excluding options). Depending on whether the appropriation is “no-year” money or money with a definitive expiration, such commitments can be problematic;

Automatic renewals – contract or purchase order clauses that provide that the agreement will automatically renew upon its termination unless an action is taken. This type of provision is always problematic;

Indemnification clauses – contract or purchase order clauses that obligate the Commission to indemnify other parties against losses without limitation (“open ended” indemnification” clauses). This type of provision is never permitted; and

Unauthorized/Improper Purchases – FCC funded purchases of goods or services that are generally prohibited by appropriations law (*e.g.*, personal items, mementos and similar presentation items distributed to either FCC employees or individuals outside the Commission, food and water, motor vehicles).

Note: For credit programs, OMB Circular A-11 provides that the FCC is required to report Antideficiency Act violations for the over-obligation or over-expenditure of (a) the subsidy, (b) the credit level supportable by the enacted subsidy, (c) the amount appropriated for administrative expenses, (d) the expired unobligated balance of the subsidy, and (e) the apportioned borrowing authority in a financing account.

8. PENALTIES:

- A. The criminal penalty for an officer or employee knowingly and willfully violating the Act is a fine of not more than \$5,000, imprisonment for not more than two years, or both.
- B. The administrative penalty for violations of the Antideficiency Act, as noted in OMB Circular A-11, is appropriate administrative discipline, including, when circumstances warrant, a written reprimand, unsatisfactory performance rating, transfer to another position, suspension from duty without pay or removal from office. Corrective action and administrative discipline will also be taken, as needed for correction and prevention of other violations of administrative subdivision of funds that are not violations of the Antideficiency Act. This would include not adhering to the policies and procedures as noted within this directive.

9. REPORTING VIOLATIONS:

The Antideficiency Act provides that if an officer or employee of an executive agency violates its key provisions, the head of the agency shall report immediately, through OMB to the President and Congress and to Comptroller General all relevant facts and a statement of actions taken. OMB Circular A-11, Section 145, "Requirements for Reporting Antideficiency Act Violations," Subsection 7, "How do I report a violation?" describes the reporting process. Early reporting of any potential violation of the Antideficiency Act can help avoid or curtail an actual violation and is therefore an important element of the administrative control of funds.

The Commission's CFO shall have authority to investigate potential or actual violations of the Antideficiency Act and all other statutes and regulations related to the obligation and expenditure of funds in this or any other Acts. The CFO shall determine whether violations exist; and shall submit final reports on violations to the Chairman. The Commission's process for the disclosure, review, reporting, and action on potential and actual violations is as follows:

- A. Notification of Possible Violations: Any Commission employee having knowledge of a possible Antideficiency Act violation must immediately notify the CFO about the activity in question. The employee should provide information and documents that support their belief that a possible Antideficiency Act violation exists.
- B. Referrals. If the Office of Inspector General (OIG), OMB, or GAO informs the Commission that there may be a possible Antideficiency Act violation, the CFO will consider the information as a referral that needs to be investigated, and if determined to be a violation, will explain why he or she had not previously discovered and reported the violation prior to the external notification.
- C. Establishing a File and Review Team. The CFO will maintain a file on each alleged Antideficiency Act violation that will include reports documenting action taken to review and address the issue. The CFO will assign employees to a review team that will investigate the potential Antideficiency Act violation. The CFO will assist the review team in carrying out their responsibilities throughout the review process. The review team should consist of staff who are independent of the activity in question. The review team may consult with, or obtain the assistance of, the Office of General Counsel and

such other officials as the review team determines necessary to carry out its duties. All Commission employees are required to cooperate with the review team in their investigations of potential Antideficiency Act violations.

D. Preliminary Assessment:

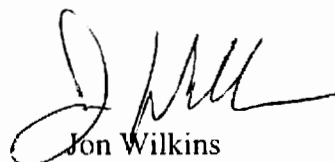
- (1) The CFO will conduct a preliminary assessment of any alleged violation and determine whether a possible Antideficiency Act violation exists.
- (2) Throughout the review process, the CFO will make every effort to ensure that no funding or disbursement actions are taken that might continue or compound any violation.
- (2) If the preliminary assessment clearly determines that there is no violation, the CFO will document the file that an Antideficiency Act violation was alleged, but a determination was made that there is no such violation, with the basis for the determination. If, however, the notification of violation comes from OIG, GAO or OMB, the agency must follow the reporting procedures detailed below even if the agency determines that there is no violation. In that event, the report will explain the basis for the agency's determination of no violation.
- (3) Whenever the CFO's preliminary assessment identifies opportunities for improvements in funds control, the CFO's findings will be forwarded to all program areas concerned.
- (4) After the CFO completes a preliminary assessment and determines that there is a possible Antideficiency violation, the CFO will notify the Chairman of a possible violation in writing and explain the basis of the need for further review. A copy of the notification should be sent to the General Counsel.

B. CFO Final Assessment to Determine Whether an Antideficiency Act Violation Occurred: The CFO will further review, gather additional information, and prepare a report that will serve as the Chairman's report under the Antideficiency Act. If the review determines no violation occurred, the CFO will issue a report to the Chairman and General Counsel advising them of the finding and supporting facts. If, however, the notification of violation comes from OIG, GAO or OMB, the agency must follow the reporting procedures detailed below even if the agency determines that there is no violation. In that event, the report will explain the basis for the agency's determination of no violation. If the review determines that a violation did occur, then the CFO will take three actions (may be concurrent) before it issues a final report. First, the CFO will provide due process to the official or officials viewed as responsible for the violation of the Antideficiency Act, allowing them an opportunity to provide comments that may impact the final report of the investigation. Second, the supervisor(s) of the employee(s) responsible for a violation will be consulted on the violation to recommend disciplinary action to the CFO. Third, the CFO will provide a copy of the draft report to the Chairman and General Counsel to allow them an opportunity to review and provide comments.

The final report of the violation must describe all pertinent facts of the Antideficiency Act violation, including the position of the employee² responsible (and any disciplinary action), and make recommendations on corrective actions that should be taken to preclude a recurrence. If the review determines that a violation did occur and possible criminal activity is suspected, the CFO will refer such activity to the Inspector General for a criminal investigation and the CFO will proceed with the review and report process in coordination with the criminal investigation of the Inspector General.

- C. Final Report: The CFO shall submit a report on violations to the Chairman. The Chairman will send the final report to the President, OMB and the Congress in accordance with applicable statutes and OMB circulars. On the same date, the CFO will provide GAO, the General Counsel and any other appropriate officials with a copy of the final report. Any recommended penalties will be imposed on the person(s) determined to be responsible for the violation and any other recommendations or corrective actions in the final report will be implemented by the Commission.

10. ACCOUNTING SUPPORT FOR FUND CONTROL SYSTEMS: See appendix B, *infra*.
11. APPORTIONMENT PROCEDURES: – See appendix A, *infra*.
12. POLICY ON ALLOTMENTS AND SUBALLOTMENTS: – See appendix A, *infra*.
13. TREATMENT OF ANTICIPATED BUDGETARY RESOURCES ALREADY ENACTED INTO LAW: See appendix A, *infra*.
14. DEFICIENCY APPORTIONMENTS: See appendix A, *infra*.


Jon Wilkins
Managing Director

² OMB Circular A-11, Section 145, was revised in 2015 to delete the requirement to identify the responsible individual by name in the final report.

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Standards and Process for Holding Disbursements to Beneficiaries and Service Providers.	
	Directive Number: FCCINST 1038.1	Effective Date: April 2016

- 1) **PURPOSE:** This directive sets forth the Federal Communications Commission's (Commission or FCC) policies, procedures, and responsibilities regarding when and how the Commission may direct the Administrator of the Universal Service Funds (USF Administrator or Administrator) to hold commitments to beneficiaries and service providers for the following universal service fund (USF) programs: Connect America Fund (CAF) and Lifeline.
- 2) **SCOPE:** This directive applies to all Bureaus and Offices within the FCC. It does not apply, however, in the event that a different process has been established by rule or Commission order to govern particular categories of cases.
- 3) **DEFINITIONS:**
 - a) "Credible information" means information from any source including but not limited to:
 - i) Information received during the course of the Commission's own investigation or audit; an investigation or audit performed by another governmental entity; an investigation or audit by the Administrator; or an audit conducted by the funding recipient;
 - ii) The filing of local, state or federal criminal charges, civil fraud charges, or qui tam suits;
 - iii) Information received from the media, State governmental agencies, Congress, local, state or federal law enforcement.
 - b) "Federal Do Not Pay List" was created by Executive memorandum and requires agencies, before payment and award, to check the following existing databases (where applicable and permitted by law) to verify eligibility: the Social Security Administration's Death Master File, the General Services Administration's Excluded Parties List System, the Department of the Treasury's Debt Check Database, the Department of Housing and Urban Development's Credit Alert System or Credit Alert Interactive Voice Response System, and the Department of Health and Human Services' Office of Inspector General's

List of Excluded Individuals/Entities. This network of databases, and additional databases so designated by the Director of the Office of Management and Budget (OMB) in consultation with agencies, is collectively known as the "Do Not Pay List." *See* 75 FR 35953.

- c) "Good Cause" not to hold payments or to hold payments only in part may include, but is not limited to, interference with law enforcement investigations; considerations involving life, property, or national security emergencies; or a detrimental effect on continuity of service to a substantial number of customers or end users.
- d) "Red light" rule requires the Commission to withhold action on applications and other requests for benefits when the entity applying for or seeking benefits has a delinquent balance due to the Commission, or its components (USF, Telecommunications Relay Service (TRS), Local Number Portability (LNP), and North American Numbering Plan (NANP)). *See* 47 C.F.R. § 1.1910. The red light list is a list maintained by the Commission of such entities. *See* Red Light Display System Login, Federal Communications Commission, available at www.fcc.gov/redlight/.
- e) "Payment" and "funding" are used interchangeably in this directive to refer to the disbursement of funds to USF recipients.
- f) "Hold" means the withholding of USF funds to an entity after the application of the standard found herein.

4) STANDARD:

- a) The Commission may direct the Administrator to hold payment, either wholly or in part, when any of the offices or bureaus of the Commission has proof, or credible information, that leads it to reasonably believe, based on the totality of the information available, that all or part of a payment would be in violation of the statutes and regulations applicable to the USF programs. In deciding whether to hold payment, the Commission will consider the factors set forth at section 5 below. The Commission will also consider whether there is good cause not to do so, or to hold only in part.
- b) The Commission must direct the Administrator to hold payments when an entity is delinquent in non-tax debts owed to the Commission or its components, i.e. the entity is on the Commission's red light list.
- c) The Commission may direct the Administrator to hold payments when an entity is on the Federal Do Not Pay List. *See* Do Not Pay, Department of Treasury, Bureau of the Fiscal Service, available at <http://www.donotpay.treas.gov/>.

5) ADDITIONAL CONSIDERATIONS AFTER STANDARD IS MET:

- a) After determining that the standard articulated in (4)(a) is met, the Commission staff will consider, among other things, the following factors in determining whether to hold funding and in establishing the parameters of the hold of funding:
 - i) the weight of the evidence that significant program violations, or program waste, fraud, or abuse, is occurring and has resulted, or will result, in overpayments to the particular recipient;
 - ii) whether the issue appears to be widespread (that is, industry-wide), or isolated to a particular recipient;
 - iii) whether the issue is a systemic part of a recipient's operations or limited in scope to a particular geographic area or business unit;
 - iv) whether a full or only partial hold of funding is warranted;
 - v) the amount of money at stake;
 - vi) the impact of a funding hold on the recipient; and
 - vii) the precedential impact of holding funding.

6) COMMISSION PROCESS:

- a) Commission staff shall coordinate on whether a funding hold is warranted in a particular case and shall bring the case to the Wireline Competition Bureau Chief and the Enforcement Bureau Chief if staff believe that a hold may be appropriate.
- b) The Wireline Competition Bureau Chief and the Enforcement Bureau Chief shall decide whether the known facts meet the standard articulated in section 4(a). The Wireline Competition Bureau Chief and the Enforcement Bureau Chief will have authority to hold funding of USF disbursements (subject to consultation with the General Counsel as described below at (d)). If there is disagreement between the Bureau Chiefs on whether to hold funding, they will raise the issue with the General Counsel for final resolution.
- c) Before any hold is implemented, the Enforcement Bureau will coordinate with the Inspector General and/or the Department of Justice as necessary.
- d) The Bureaus recommending the decision to hold funding shall provide to the Office of General Counsel (OGC) a draft letter as described in section 7 (b) below. OGC staff will review for potential litigation risk and compliance with fiscal law. If the General Counsel believes, after review of the letter, that a hold of funding may not be justified, then the Chiefs of EB and WCB and the General Counsel will consult to determine an appropriate outcome.
- e) In the event that a decision is made to hold funding, the Bureau that initiated the hold request will send the letter to the Chief Financial Officer (CFO), or his designee, who will (1) provide written direction to the Administrator to hold funding to the funding recipient; (2) issue a letter or direct USAC to issue a letter to the funding recipient to provide notice that the next (and subsequent disbursement or some portion thereof,) will be withheld. USAC will be instructed to accept such instructions only from the CFO, no other FCC staff is authorized to relay a decision directing USAC to hold funding.

7) NOTICE:

a) Timing of Notice:

- i) The Commission or the Administrator, at the direction of the Commission, shall provide notice and an opportunity for the affected party to respond prior to implementing the funding hold, except in extraordinary cases where advance notice would likely cause significant harm to the Fund, for instance, by hindering the possibility of recovering funds. The Commission or the Administrator will generally provide the recipient 30 days to respond.
- ii) If the Chief of the Bureau that initiated the hold request believes that a hold without prior notice is appropriate under (i) above, he/she will consult with the General Counsel so that they may determine an appropriate outcome. If they reach a decision that hold without prior notice is warranted, then the Commission or Administrator may hold funding prior to such notice. In such cases, the Commission or the Administrator shall provide notice simultaneously with or as soon as possible after the decision to hold funding has been communicated to the Administrator, but no later than 15 days after the funding was expected to have been disbursed.

b) Contents of Notice. The Notice shall:

- i) State that the next (and if appropriate, subsequent) disbursement, or some portion thereof, will be withheld;
- ii) Explain that the Commission has become aware of credible information suggesting that payments would be in violation of Commission rules or otherwise improper, and has determined, based on the totality of the information available, that payment would likely not be consistent with program rules, and that funding should be held pending completion of further investigation;
- iii) Provide the factual basis for the determinations in (ii) at a level of specificity that gives the recipient an opportunity to provide evidence or argument to the contrary, without compromising any pending law enforcement investigations, and that will allow OGC to defend the decision in court if necessary;
- iv) Give the recipient an opportunity to attempt to demonstrate why the payments should not be held. If possible, the letter should explain the type of response that could, if submitted quickly enough, resolve the issue and avoid the need for holding of payments;
- v) Without compromising any pending law enforcement investigations, describe the factual basis for the hold at a level of specificity that provides the recipient an opportunity to respond to the allegations;
- vi) Provide thirty (30) days for the funding recipient to respond to the notice. The beneficiary or service provider response shall be sufficiently detailed to provide the Commission and Administrator with the information necessary to evaluate whether there has been a violation of the USF program rules;
- vii) Explain that the Commission may direct the Administrator to recover from the beneficiary or service provider past funding that is found to have been disbursed in violation of the USF program rules; and

viii) Explain that if the beneficiary or service provider does not respond to the Commission's letter and requested information therein, the requested funding may be denied permanently.

- c) If the funding recipient does not persuade the Commission that the hold should be lifted, then the Commission or Administrator will notify the beneficiary or service provider of its decision as soon as practical, but not to exceed one (1) month from the date of the decision to continue to hold funding.
- d) If the funding recipient does persuade the Commission that the hold should be lifted, then the Commission will promptly direct USAC to do so using the procedures set forth below.

8) DURATION OF FUNDING HOLD:

- a) Funding will be held as set forth by the process set forth above, but generally not to exceed one (1) year. If, after one (1) year, the Commission determines that there is additional credible information to hold for longer than one (1) year, it will notify the funding recipient using the process outlined in section 7, above. In determining whether to continue to hold funds after one (1) year, the Commission will consider the same factors set forth above for determining whether to implement an initial hold.

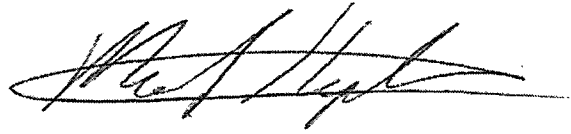
9) RELEASING A FUNDING HOLD:

- a) To release a funding hold, the Wireline Competition Bureau Chief and/or the Enforcement Bureau Chief as appropriate shall notify the Chief Financial Officer, or his or designee, of the decision to release funding.
- b) The Chief Financial Officer shall:
 - i) Provide written direction to the Administrator to release the funding hold to the funding recipient.
 - ii) Inform the funding recipient that the funding hold has been released, or direct the Administrator to do so.

10) TRACKING: The Administrator shall maintain a list of all funding withheld by the Commission and provide such list, by program, to the Commission, including the Office of Managing Director, the Wireline Competition Bureau, and the Enforcement Bureau on a monthly basis. This list will include at a minimum:

- a) name and location of beneficiary and/or provider;
- b) month and funding year at issue (if relevant);
- c) date that the decision to hold funding was made;
- d) applicable FCC Form numbers associated with funding request;
- e) reason for the funding hold;
- f) date of notice to beneficiary and/or provider;
- g) one year deadline for the funding hold;

- 11) EFFECTIVE DATE AND IMPLEMENTATION: This directive is effective immediately and shall be implemented promptly upon distribution.

A handwritten signature in black ink, appearing to read 'Mark Stephens', with a long horizontal flourish extending to the right.

Mark Stephens
Acting Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Prompt Payment Procedures	
	Directive Number FCCINST 1040.3	Effective Date April 2016

1. PURPOSE:

To supplement the Prompt Payment rules as implemented by 5 CFR Part 1315 by detailing the Federal Communications Commission's ("FCC" or "Commission") responsibilities.

2. AUTHORITY:

- a. The Prompt Payment Act 31 U.S.C. §§3901-3907, as implemented in 5 CFR Part 1315.
- b. The Contracts Disputes Act of 1978 (41 USC § 601).
- c. Federal Acquisition Regulation, 48 CFR Subpart 32.9.
- d. Treasury Financial Manual (TFM) Volume 1 Part 4A Chapter 2000 (Overall Disbursing Rules for Federal Agencies).

3. BACKGROUND:

The Prompt Payment Act (Act) requires Federal agencies to pay bills on time, to pay interest and additional penalties when payments are late, and to take discounts only when payments are made within the discount period. Implementation of the Act is intended to result in timely payments, better business relationships with suppliers, improved competition for Government business, and reduce costs to the Government for goods and services. Implementation must be consistent with sound cash management practices and related Treasury regulations.

4. POLICY:

The Commission will comply with the requirements of 5 CFR Part 1315 and will make payments as close as possible to, but not later than, the due date. Payments will be based on the receipt of a proper invoice in the designated billing office and satisfactory performance of contract terms. Payments made after the required due date may be subject to interest penalties. Discounts taken after the applicable discount period has expired may be subject to interest penalties. Interest penalties paid without the vendor requesting them will be absorbed within the funds available to the Commission each fiscal year. Additional funds may not be requested to cover interest penalties incurred because of late payments.

5. RESPONSIBILITIES:

- a. Managing Director: The Managing Director is responsible for the administrative management of the Prompt Payment program at the Commission.
- b. Associate Managing Director – Financial Operations: The Associate Managing Director for Financial Operations, the Commission's Chief Financial Officer (CFO), under authority delegated by the Managing Director, is responsible for ensuring that all payment documents are processed in accordance with the Prompt Payment Act 5 CFR Part 1315, including the following:
 - (1) Issuing internal procedures. Ensuring that internal procedures will include provisions for monitoring the cause of late payments and any interest penalties incurred, taking necessary corrective action, and handling inquiries.
 - (2) Internal control systems. Ensuring that effective internal control systems are established and maintained as required by Office of Management and Budget (OMB) Circular A-123, "Management's Responsibility for Internal Control."
 - (3) Financial management systems. Ensuring that financial management systems comply with OMB guidance.
 - (4) Timely payments and interest penalties. Ensuring timely payments and payment of interest penalties where required. (Accelerated payments are implemented subject to OMB guidance)
- c. Enterprise Acquisition Center (EAC) :
 - (1) That sufficient information is contained on procurement documents to establish adequate documentation for prompt payment, to prevent late payment and associated interest and to take discounts where appropriate. Contracts shall contain the appropriate payment Federal Acquisition Regulation (FAR) Clauses and instructions to comply with the Prompt Payment FAR Part 32.9 regulations, policies and procedures.
 - (2) Establish contracts/purchase orders document in EAC procurement database system and attach a signed copy of the contract/purchase order to the document within the EAC procurement database system immediately upon award.
 - (3) Periodically assessing operational programs.
- d. Assistant Bureau Chiefs for Management (ABCs):

 - (1) Ensuring that all goods and services that are received by their staffs and for which they have responsibility are in good working order and/or meet the terms of the purchasing contract. All required receiving reports and/or invoice approval forms are to be forwarded to the appropriate office within three (3) work days after

receipt unless separate arrangements are made. Invoices go directly to TOG for payment.

- (a) The goods or services received must be inspected within five (5) business days of receipt and if found to be acceptable, the receiving report (Optional Form 347 (REV 6/95) Back) should be certified by the designated receiving official or Contracting Officer's Representative. A copy should be sent to TOG.
 - (b) The goods or services received must be inspected within five (5) business days of receipt and if found to be in error, with defect or other impropriety, the receiving report should **NOT** be signed. A copy of the receiving report should be sent to the Enterprise Acquisition Center (EAC) along with a short explanation of why the goods or services are not acceptable. The B/O designated receiving official should **NOT** contact the vendor without notifying the EAC and advising them of any and all discrepancies. After notification has been given to the EAC, the receiving official should prepare a written notification to the vendor advising that payment may be delayed and that the 30-day or specific contract payment date may be canceled. Following resolution of the problem, forward form A-105 to TOG.
- (2) Designating, in writing, a specific staff member (designated receiving official) and alternate to coordinate and monitor the purchasing and receipt cycles within the B/O. This individual should be familiar with all outstanding purchase orders and contracts and be able to act as a contact person with the EAC and TOG within 15-days of receipt of this directive.
 - (3) Ensuring that the performance standards, performance contracts and appraisals of affected responsible employees contain the necessary language to ensure that these requirements are met.
 - (4) Working with TOG to correct areas of late processing of documents and taking necessary corrective or disciplinary action, as appropriate.

e. Financial Operations - Travel and Operations Group (TOG):

- (1) Establish procedures to ensure that:
 - (a) Payment documents are processed in a timely manner. (5 CFR Part 1315).
 - (b) Discounts are taken only when payments are made within the discount period. Discounts taken after the applicable discount period has expired may be subject to an interest penalty. (5 CFR §1315.4(c)(2)).
 - (c) Interest penalty calculations, if applicable, are consistent with 5 CFR §1315.10.
-
- (2) Return an improper invoice to the vendor explaining the rejection reason(s).
 - (a) Taxpayer identification number.

- (b) Vendor name, invoice number, account number, and/or any other identifying number agreed to by contract.
 - (c) Banking information, unless agency procedures provide otherwise, or except in situations where electronic funds transfer (EFT) requirement is waived under 31 CFR § 208.4.
- (3) Establish a program for monitoring the causes of interest penalties incurred and discounts lost, and take necessary action to improve the performance of personnel at fault including corrective or disciplinary action, as appropriate, (5 CFR §1315.3(a)).
- (4) Research interest penalties that exceed \$25.00 and determine the reason(s) for the late payment(s). A letter will be sent to the designated Contracting Officer's Representative (COR) and COR supervisor notifying them of the penalty and the reason(s).
- f. Financial Operations - Financial Systems Operations Group (FSOG): The FSOG Chief is responsible for establishing financial management systems to provide complete, timely, reliable, useful and consistent financial management processes, information and reports as required by OMB guidance.
- g. Office of Inspector General: Office of The Inspector General responsibilities include ensuring that the Inspector General and his or her staff or contractors review payment performance and system accuracy, consistent with the Chief Financial Officers (CFO) Act requirements. (5 CFR § 1315.3(d)).



Mark Stephens
Acting Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Program Time Reporting and Cost Allocation	
	Directive Number: FCCINST 1053.4	Effective Date: August 2016

1. **PURPOSE**: To provide guidance, policy and procedures concerning the implementation and maintenance of program codes used in the Federal Communications Commission's (FCC or Commission) core financial management system, also known as Genesis. Genesis integrates time reporting and cost accounting to meet the Commission's strategic and performance goals.
2. **CANCELLATION**: This instruction replaces FCC INST 1053.3, dated December 2, 2014.
3. **SCOPE AND APPLICABILITY**: This directive applies to all Bureaus and Offices.
4. **AUTHORITY**:
 - a. Government Performance and Results Modernization Act of 2010, Public Law 111-352 (GPRA Modernization Act)
 - b. Office of Management and Budget (OMB) Circular A-11
 - c. The Accountability of Tax Dollars Act of 2002, Public Law 107-289, 31 U.S.C. § 3515
 - d. Statement of Federal Financial Accounting Standards (SFFAS) No.4, Managerial Cost Accounting Concepts and Standards for the Federal Government
 - e. Statement of Federal Financial Accounting Standards (SFFAS) No.7, Accounting for Revenue and Other Financing Sources
5. **DEFINITIONS**:
 - a. **Cost Allocation**. The process of allocating to individual program codes the cost of employee time and non-payroll expenses such as travel, training, services and supplies, reimbursable work agreements, contractor support, and information technology.
 - b. **Fund Code**. Fund codes are seven- or eight-digit internal identifiers for the Treasury symbols to be charged or credited for agency disbursement or receipt transactions. Fund codes are linked to a specific purpose. For example, fund X54_0100 currently serves as the code associated with accounting for receipts and expenditures under the auction program.

- c. Genesis. The Commission's core financial system, which includes a cost accounting module.
 - d. Output Indicator. A type of measure, specifically the tabulation, calculation, or recording of activity or effort, usually expressed quantitatively. Outputs describe the level of product or activity that will be provided over a period of time. While output indicators can be useful, there must be a reasonable connection between outputs used as performance indicators and outcomes. Output indicators are based on evidence supporting the relationship between outputs and outcomes, or in the absence of available evidence, based on a clearly established argument for the logic of the relationship. For example: An output indicator may be the quantity of products or services delivered by a program, such as the number of inspections completed or the number of people trained.
 - e. Outcome Indicator. A type of measure that indicates progress against achieving the intended result of a program. Indicates changes in conditions that the government is trying to influence.
 - f. Performance-Based Cost Accounting System. A Performance-Based Cost Accounting System captures the agency's costs and assigns them to program codes on both a direct and indirect basis according to the consumption of agency resources.
 - g. Performance Goals. A statement of the level of performance to be accomplished within a timeframe, expressed as a tangible, measurable objective or as a quantitative standard, value, or rate. For purposes of OMB Circular A-11 and implementation of the GPRA Modernization Act, a performance goal includes a performance indicator, a target, and a time period. The GPRA Modernization Act requires performance goals to be expressed in an objective, quantifiable, and measurable form unless agencies in consultation with OMB determine that it is not feasible. In such cases, an "alternative form" performance goal may be used. The requirement for OMB approval of an alternative form goal applies to performance goals only. Milestones are often used as the basis of an alternative form performance goal. Performance goals specified in alternative form must be described in a way that makes it possible to discern if progress is being made toward the goal.
 - h. Program Code. The four-digit numeric code assigned to a particular activity contained in the FCC's performance budget.
 - i. Strategic Goal. A statement of aim or purpose that is included in a Strategic Plan. Strategic goals are identified with one alpha character. Strategic goals articulate clear statements of what the agency wants to achieve to advance its mission and address relevant national problems, needs, challenges and opportunities. These outcome-oriented strategic goals and supporting activities should further the agency's mission.
6. BACKGROUND: In order to comply with applicable Federal legislation and guidance regarding the development and submission of its annual budget to OMB and Congress, program time reporting and cost allocation functionality is integrated into Genesis. The system is designed to support the Commission's emphasis on implementing good

management practices by accurately accounting for the use of its resources and allocating costs in accordance with the Commission's strategic plans and goals.

7. POLICY:

The Commission will:

- a. Record employee time and attendance on a program basis;
- b. Capture non-payroll costs to programs by requiring that program codes be included on all expense related transactions;
- c. Capture and report the full cost of conducting business across its long-term strategic and annual performance goals; and
- d. Perform an annual review of all active program codes.

8. RESPONSIBILITIES:

A. The Commission's Chief Financial Officer (CFO) or his/her designee overseeing the establishment and proper use of program code and strategic goal reporting is responsible for:

- (1) Approving or denying requests for a program code. Criteria for acting upon requests for new program codes should include, but are not limited to:
 - (a) The extent of its association with the strategic goals in the Commission's strategic plan and/or the performance output indicators included in the Commission's annual performance plan. The Commission's current strategic plan and annual performance plan are available online at: <http://www.fcc.gov/encyclopedia/fcc-strategic-plan>;
 - (b) Whether the requested program code is broad enough to apply to the needs of multiple bureaus; and
 - (c) Whether the requested program code represents a significantly new initiative or management interest that should be tracked and reported separately.
- (2) Conducting a comprehensive review of program codes to ensure that they reflect and align with any changes to the FCC's strategic goals. This review will take place following issuance of a new FCC Strategic Plan.
- (3) Reviewing requests for new or amended program codes, and assigning and tracking approved program codes.
- (4) Notifying B/Os of the approval or denial of program codes.

B. The Financial Systems Operations Group (OMD-FO-FSOG) is responsible for:

- (1) Entering new program codes into the appropriate financial systems.
- (2) Notifying the Bureaus and Offices (B/Os) when approved program codes are entered into the financial systems and are available for use.
- (3) Generating management reports on program codes.
- (4) Ensuring that only valid program codes are maintained in the financial systems.
- (5) Removing and deleting outdated program codes.
- (6) Coordinating with Human Resources Management (HRM) for guidance to staff on the use of program codes as part of their ongoing WebTA training and outreach within the Commission.
- (7) Updating the appropriate reference material(s) on the FCC intranet website to incorporate newly assigned codes.

C. The Bureaus/Offices are responsible for:

- (1) Originating requests for creating and deleting program codes as needed.
- (2) Identifying the strategic goal(s) that a program supports.
- (3) Identifying the output or outcome indicators (programs) that the requested code is to be associated with.
- (4) Developing the program titles.
- (5) Providing a specific definition of a new program and its purpose, including example activities.
- (6) Establishing a program's life cycle (the period in which the program code will be active).
- (7) Providing justification that supports the request to create or delete a program code.
- (8) Coding all financial documents with the appropriate program codes.

9. PROCEDURES: The following processes are applicable to all B/Os within the FCC that desire to request new codes or request deactivation of existing codes.

A. In order to establish and add a new program code, the proposed program code must:

- (1) Be defined as an output or outcome indicator in the performance budget;

- (2) Require more than 160 hours to accomplish;
 - (3) Require more than one person to complete the task; and
 - (4) Be expected to last longer than two pay periods.
- B. Requests for an exception or waiver of the criteria contained in section 9.A., above, shall be directed to the CFO or his/her designee.
- C. For each new program code requested, the originator of the request must:
- (1) Provide advance notice of the request as early as possible but no later than two pay periods prior to the need for the new code when feasible;
 - (2) Identify the FCC strategic goal that the program supports;
 - (3) Develop a program title that will identify the program;
 - (4) Create a description for the program that synthesizes the purpose of the program;
 - (5) Identify some activities that represent the kind of work performed in support of the program;
 - (6) Identify all the different fund codes that could be associated with the program (*e.g.*, X01– Appropriations Funded, X54 – Auctions Funded, 091 – Reimbursable Work Agreements, *etc.*);
 - (7) Estimate beginning and ending dates during which the program code will be active (*e.g.*, March 3, 2014 to March 3, 2015); and
 - (8) Provide a justification for the establishment of the program code.
- D. The originator of the request must submit the request via a memorandum or email to his/her supporting Assistant Bureau Chief for Management (ABC) or equivalent. The request must incorporate all the information identified in sections 9.A., B., and C. above. The ABC has the responsibility to coordinate the request with their B/O management for review and approval.
- E. Once the request is approved by the B/O Chief or his/her designee, the ABC incorporates any change recommendations into the memorandum or email and forwards it to the Deputy CFO, Financial Systems (Deputy CFO), who in turn will forward the request to the CFO or the individual designated by the CFO as the approving official for additions or deletions to program codes.
- F. The CFO or his/her designee makes a determination to either approve or deny the request. If approved, the Deputy CFO directs the Financial Systems Operations Group to complete the following:

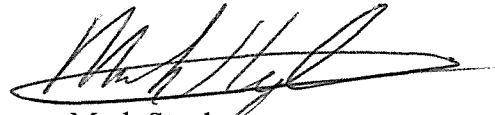
- (1) Assign a five-digit alphanumeric code consistent with the existing coding structure;
- (2) Enter this code into the appropriate financial systems (*i.e.*, Genesis) and WebTA;
- (3) Notify the requestor that the code is active and available for use; and
- (4) Update the appropriate reference material(s) on the FCC Intranet website to include the new code(s).

G. Denial of Request. If the CFO or his/her designee denies the request for a new program code, the decision shall be communicated to the requesting ABC along with an explanation why the request was denied.

H. Deactivation of Program Codes. A request to deactivate an existing program code is reviewed by the CFO or his/her designee to verify that work on a specific program has ended, its costs no longer require tracking, and that it is not needed to support management reporting.

- (1) For each request to deactivate a program code, the originator of the request must:
 - a. Identify the existing title and code for the program;
 - b. Provide a justification for why this program code is no longer needed; and
 - c. Provide the proposed effective date of the deactivation.
- (2) The originator must submit the request to the supporting ABC or equivalent via a memorandum or email. The request must include all the information identified in section 9.H.1, above. The ABC has the responsibility to coordinate the request with their B/O management for review and approval.
- (3) If the request is approved by B/O management, the ABC incorporates any recommendations into the memorandum or email and forwards it to the Deputy CFO, Financial Systems, who in turn will forward the request to the CFO or the individual designated by the CFO as the approving official for deletions to program codes.
- (4) The CFO or his/her designee reviews the request. If approved, the Deputy CFO directs the completion of the following by the Financial Systems Operations Group:
 - a. Removal of the code from the proper systems (*i.e.*, Genesis) and WebTA;
 - b. Informing the requesting B/O and other affected B/Os that the request has been approved; the code has been deactivated in the proper systems, and is no longer available for use; and

- c. Updating the appropriate reference material(s) on the FCC Intranet website to remove the deactivated code(s).

A handwritten signature in black ink, appearing to read 'Mark Stephens', with a large, sweeping horizontal stroke underneath.

Mark Stephens
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	CORES/FCC Registration Number	
	Directive Number FCCINST 1058.3	Effective Date March, 2015

1. **PURPOSE:** To provide guidance concerning the implementation and management of the Commission Registration System (CORES) and to establish responsibility for the maintenance, and related financial matters.
2. **AUTHORITY:**
 - a. The Debt Collection Improvement Act of 1996 (DCIA), Public Law 104-134, 110 Stat. 1321-358 (April 26, 1996), enacted as Section 31001 of the Omnibus Consolidated Rescissions and Appropriations Act of 1996 (31 USC §§ 3711 *et. seq.*).
3. **BACKGROUND:** CORES is designed to track and record the issuance of the FCC Registration Number (FRN). The FRN enables the agency to determine whether the holder has any delinquent debt by linking the FRN to the Tax Payer Identification Number (TIN) in order to be in compliance with the DCIA. The DCIA requires anyone doing business with the Federal government to provide their TIN issued by the Internal Revenue Service (IRS). The TIN is used to identify entities owing Federal debt; therefore, an FRN will not be issued to an entity without receiving their TIN.

Because the TIN is personally identifiable information with privacy protection considerations, the Commission requires persons or entities doing business with the Commission and its reporting components (Universal Service Fund (USF), North American Numbering Plan Administration (NANP), Telecommunications Relay Service (TRS), *etc.*) to obtain an FRN.

This directive does not address the question of how the FRN will be used to determine whether persons or entities doing business with the Commission have outstanding delinquent debts or what action will be taken against those applicants or entities. The procedure of handling applications or filings by persons or entities with non-tax delinquent debt owed to the Commission or the Federal government is addressed in FCC INST 1064.3 – Debt Collection.

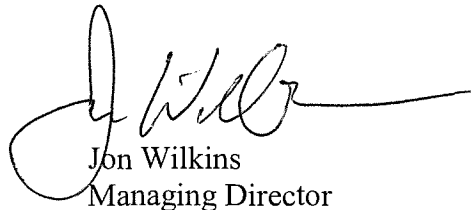
4. **POLICY:** The Commission will:
 - a. Maintain a link between the TIN and the FRN.
 - b. Require the submission of the FRN on all feeable and non-feeable filings and applications, including those filings with USF, NANPA, and TRS, which may result in the grant of a benefit.
 - c. Require the mandatory use of the FCC Form 159 (Remittance Advice) for all payments, except those payments accompanied by an invoice or payment order.

- d. Check to see if an applicant has an outstanding delinquent auction debt existing on the Commission's records.
 - e. Check to see if applicants interested in participating in the auction program have ever defaulted on debts or loans owed the Commission.
 - f. Establish procedures that provide assurance that fees have been paid prior to the grant of any request for benefit.
 - g. Deactivate a FRN when discovered that an incorrect TIN has been used in CORES.
 - h. Notify both parties when an FRN is deactivated due to an incorrect TIN recording in CORES. If multiple parties (FRNs) are sharing the same TIN, the Office of Managing Director/Financial Operations (OMD/FO) will notify the FRN and the TIN holder's that the FRN is being deactivated.
 - i. Eliminate repetitive collection of data.
 - j. Improve the Commission's mechanism for properly recording and tracking receipts made to the Commission.
 - k. Not return a payment of a civil monetary penalty or an outstanding accounts receivable.
 - l. Require that individual users log in with unique User IDs in order to identify who is acting upon an FRN.
5. RESPONSIBILITIES: The Commission is required to assure compliance with DCIA. In furtherance of this requirement:
- a. The OMD/FO is responsible for:
 - (1) Collecting all delinquent debts, and for monitoring collections.
 - (2) Compiling the files necessary for transmission to the Treasury and for referral of delinquent debts to the Treasury.
 - (3) Maintaining a link between the FRN and the TIN.
 - (4) Implementing a system that compares outgoing refunds as possible offset for outstanding delinquent debt.
 - (5) Contacting and coordinating resolution with applicants, licensees, or regulatees who are delinquent on a debt. The Genesis core financial system (Red Light Display System) will respond when a Section 8 fee is received, and delinquent debt is recognized for that TIN and when an applicant submitting an upfront remittance is delinquent on any current or prior FCC debt.
 - (6) Providing assistance to the Bureaus and Offices on matters related to this Directive.
 - (7) Returning any applications or filings as unprocessable if the remittance advice is incomplete or obsolete.
 - (8) Processing FCC Form 160 and registering entities.
 - (9) Recording the FRN on the FCC Form 160 once registration has been completed.
 - (10) Accessing the CORES database in order to validate FRNs.
 - (11) For Section 9 (regulatory fee) payers, verifying the applicant, licensee or regulatee's fee exempt status under section 501(c) (3) of the Internal Revenue Code.
 - (12) Contacting the payer/applicant in order to secure a valid FRN if the event is related to the following activities:
 - a. Auctions;
 - b. Section 9;
 - c. Special Temporary Authority Request (STA emergency); or
 - d. Payments received against outstanding debts and civil monetary penalties.

(13) Staffing a help desk who will respond to telephone and e-mail inquiries.

b. The Bureaus and Offices are responsible for:

- (1) Reviewing applications, request for authorizations and other fee filings to ensure that the correct fee for each application has been paid prior to granting the application.
- (2) Verifying applicant, licensee or regulatee fee exempt status.
- (3) Compiling a list of specific instances in which the FRN must be provided for services under their purview.
- (4) Allow applicants a 10-business day grace period for applications that have time-critical deadlines and may be filed on paper. The filer will be notified of the omission of the FRN and informed of the deadline for submitting the correct FRN.
- (5) Allow applicants a 10-business day grace period for appearances in hearing proceedings.
- (6) Maintaining automated systems to:
 - a. Ensure that the proper fee has been received prior to the grant of any application or authorization.
 - b. Capture/validate the FRN or User ID at the time of log-on.
 - c. Incorporate the FRN into their database.
 - d. Provide an access mechanism to the CORES Web site to register a new entity for the licensing system.
 - e. Provide FRN for fee sufficiency check.
 - f. Populate the electronic FCC Form 159 with the applicant FRN.
- (7) Notify OMD if there is a Section 8 Application Fee remittance amount due for an emergency Special Temporary Authority (STA). Remittance Advice (FCC Form 159) and fees are not sent to the FCC with emergency requests for STA. The Bureau or Office will notify OMD of the amount due, and ask OMD to bill the applicant for the amount. OMD will notify the Bureau or Office when the amount is paid.
- (8) The Wireline Competition Bureau will notify tariff filers that a tariff was ineffective if and when it is discovered that the tariff fee for the service was not properly submitted or paid, and take other appropriate action.
- (9) Assigning an FRN to all outgoing civil monetary penalty payment orders, where the alleged violator is not already registered in CORES.
- (10) The Consumer and Governmental Affairs Bureau (CGB) will staff a help desk who will respond to and service Personal Security Question reset requests and will assist customers who need assistance accessing their FRN(s).



Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Communicating Spectrum Auction Events that have Financial Recording and Reporting Impact	
	Directive Number FCCINST 1059.4	Effective Date March 2, 2016

1. **PURPOSE:**

To provide guidance, policy and procedures concerning the communication of spectrum auction events that have a financial impact or result in the recording of a financial transaction.

2. **BACKGROUND:**

Since its enactment in 1993, Section 309 of the Communications Act of 1934, as amended, has authorized the Commission authority to use competitive bidding to choose from among two or more mutually exclusive applications for an initial license. The Act requires the Commission to use auctions to resolve mutually exclusive applications for initial licenses unless the Commission finds that it is in the public interest not to do so, or unless certain exemptions apply, including exemptions for public safety radio services, digital television licenses to replace analog licenses, and non-commercial educational and public broadcast stations. Since 1994, the Commission has conducted auctions of licenses for electromagnetic spectrum. These auctions are open to any eligible entity or individual that submits an application and upfront payment, and is found to be a qualified bidder by the Commission. Congress has extended and expanded the Commission's auction authority over the years. Most recently, in 2015, by the Bipartisan Budget Act of 2015, which among other things authorizes the Commission to conduct incentive auctions in which existing licensees may voluntarily relinquish their spectrum usage rights, in order to permit the assignment by auction of new initial licenses subject to flexible-use service rules, in exchange for a portion of the resulting auction proceeds.

3. **SCOPE:**

This directive, including appendix A (Pre-Auction Procedures and Timeline), applies to all Bureaus and Offices involved in the spectrum auction and post-auction licensing processes, excluding incentive auctions.

4. **RESPONSIBILITIES:**

a. The auctioning Bureaus are responsible for:

- (1) Advising the Office of Managing Director - Financial Operations - Revenue and Receivables Operations Group (RROG) of planned auction events and dates;
- (2) Notifying RROG of applicants qualified to participate in the auction;

- (3) Providing RROG with each qualified applicant's FCC Registration Number (FRN), its bidding unit eligibility, and a list of the items/markets selected on the short-form applications (FCC Form 175);
- (4) Issuing the Public Notice announcing the winning bidders and any bid withdrawal payment obligations;
- (5) Providing RROG a draft copy of the *Qualified Bidders, Closing, Prepared to Grant* and/or *Grant Public Notice*, including instructions for making payment and for completing the FCC Form 159, and a list of those licenses being granted;
- (6) Providing RROG with detailed information concerning the winning bidders, withdrawal payments, down payments, final payments and/or refunds, FCC Forms 301, 346, 349, 601, and 602 filing requirements as appropriate, requests for rule waivers that may have a financial impact or result in the recording of a financial transaction, and licensing matters that may have a financial impact or result in the recording of a financial transaction;
- (7) Notifying RROG of any unjust enrichment obligations;
- (8) Maintaining an inventory of available spectrum that is subject to auction;
- (9) Providing RROG with information on the status of applicants that are subject to higher upfront payment obligations applied to former defaulters in accordance with 47 CFR §1.2106; and
- (10) Issuing demand letters for interim or final withdrawal or default payments in coordination with RROG.

b. The Office of Managing Director - Financial Operations - Revenue and Receivables Group (- RROG) is responsible for:

- (1) Managing the day-to-day operations of the financial and accounting functions as they relate to the Auctions Program;
- (2) Coordinating all auction accounting activities, including financial accounting activities associated with individual auctions and those related to the ongoing activity associated with reviewing and managing auction-related policies and procedures;
- (3) Ensuring the credit program is maintained in accordance with Federal Credit requirements;
- (4) Serving as expert advisor in financial accounting matters to the Bureaus;
- (5) Maintaining and updating lockbox and associated bank accounts, and providing appropriate information to the auctioning Bureaus;
- (6) Accounting for upfront payments received from potential bidders, notifying the appropriate bureau(s) that all upfront payments received have been recorded in the FCC's financial system.
- (7) Ensuring that upfront payments, when applicable, earn interest through the purchase of T-Bills from the lockbox bank, in order to satisfy the requirements set forth in the Communications Act, as amended, which provides for the interest proceeds to be credited to the U.S. Treasury General Fund;
- (8) Reconciling the funds on deposit with the lockbox bank to ensure that the interest is accurate;
- (9) Processing refunds to eligible auction participants during an auction only after coordination with the auctioning Bureau;

- (10) Processing refunds to eligible auction participants after an auction;
- (11) Processing the payment of earned interest to the U.S. Treasury General Fund;
- (12) Maintaining delinquent debtor records;
- (13) Providing access to and information on delinquent debtor accounts;
- (14) Accounting for down payments and final payments received from winning bidders;
- (15) Accounting for withdrawal payments and default payments received from bidders;
- (16) Collection or compromise of auction-related debts pursuant to Part 1, Subpart O of the Commission's rules, including Sections 1.1914 and 1.1915;
- (17) Providing reports/information from the FCC's financial system (Genesis) for purposes of determining the red light status of applicants and their affiliates, and conducting research on the red light status of applicants and their affiliates;
- (18) Coordinating with the auctioning Bureaus concerning requests for waiver of payment obligations and/or payment deadlines; and
- (19) Providing the auctioning Bureaus with information on the status of payments relating to auction obligations.

5. POLICY:

- a. Bureaus and Offices will notify OMD-FO-RROG, in a timely manner, any time an auction is scheduled or of any actions that may have a financial impact; including when an auction is rescheduled to a later date, unjust enrichment payment obligations, license defaults, refunds, default and withdrawal liabilities, proposed rule changes, and payment due dates.
- b. Bureaus and Offices will seek OMD's advice and concurrence on any issues they believe may have a financial impact or result in the recording of a financial transaction.

6. REPORTING:

Once the auction is completed, information regarding spectrum auction events that have a financial impact or result in the recording of a financial transaction will be forwarded from the auctioning bureau to OMD-FO-RROG.


Jon Wilkins
Managing Director

APPENDIX A

Pre-Auction Procedures and Timeline

Purpose:

This Appendix summarizes the general framework of the policy and procedures for spectrum auctions. Listed below is the timeline that is generally followed, unless circumstances require changes, by all Offices and Bureaus that are involved in spectrum auction-related activities that have a financial impact or result in the recording of a financial transaction.

a. Comment Public Notice (Approximately 4-6 months prior to auction)

A public notice is released in accordance with the requirements of the Budget Act of 1997, seeking comment on auction procedures such as activity rules, upfront payment amounts, minimum opening bids and/or reserve prices.

b. Procedures Public Notice (Approximately 3-5 months prior to auction)

A public notice is released providing potential participants with the procedures, terms, and conditions for the auction.

c. Tutorial (Approximately 60-75 days prior to auction)

An on-line tutorial is provided to introduce potential auction applicants to the auction rules, pre-auction processes and bidding procedures. The tutorial is housed on the Auctions Internet site and can be viewed on a 24/7 basis.

d. Short-Form Application (FCC Form 175) Filing Deadline (Approximately 45-60 days prior to auction)

This is the first deadline faced by potential participants. The short-form application, which must be filed electronically, collects basic information, including the applicant's ownership structure and the items on which it wants to be able to bid during the auction. If an individual or entity does not submit its short-form application by the established deadline, it will not be able to participate in the auction.

7. Short-Form Application Status Public Notice (Approximately 30-40 days prior to auction)

After the deadline for filing, staff reviews all timely-filed short-form applications and deems them complete, incomplete, or rejected. This public notice announces the status of the applications.

The FCC sends the public notice in an overnight package to each applicant's contact person listed on the short-form application. For an applicant whose application has been deemed incomplete, a letter is included that includes a brief explanation of the omissions or deficiencies that gave rise to the "incomplete" designation. This letter also includes the name of an FCC contact person in case the applicant requires further explanation.

f. Short-Form Application Resubmission Deadline (Approximately 3-4 weeks prior to auction)

Short-form applications that were deemed "incomplete" or otherwise deficient must be corrected and refiled by this deadline, which often coincides with the upfront payment deadline.

g. Upfront Payment Deadline (Approximately 3-4 weeks prior to auction)

Potential bidders must submit a refundable deposit that is used to purchase the eligibility (bidding units) required to place bids in the auction.

h. Qualified Bidders Public Notice (Approximately 10-14 days prior to auction)

This public notice lists the bidders qualified to participate in the auction, each bidder's FCC Registration Number, and its claimed bidding credit eligibility. For some auctions, this public notice also lists each bidder's bidding unit eligibility and which items it selected on its FCC Form 175. This public notice also contains information about the mock auction, the bidding schedule for the first day of the auction, and other auction-specific details. The FCC sends this public notice to each applicant's contact person in an overnight package along with registration materials as listed below.

i. Qualified Bidders Registration (Approximately 7 days prior to auction)

Shortly after the release of the Qualified Bidders Public Notice, an overnight mailing is sent to the applicant's contact person. This mailing includes the Qualified Bidders Public Notice, RSA SecurID® tokens for logging into the FCC Auction System, the Auction Bidder Line phone number, and other materials needed to participate in the auction.

j. Mock Auction (Approximately 2-5 days prior to auction)

To ensure bidders understand the auction process, the FCC conducts a mock auction as a service to qualified bidders. The mock auction allows bidders to familiarize themselves with the bidding process and become comfortable with the rules and conduct of the auction.

k. Auction Begins

l. Auction Closes.

Approximately 2-5 business days after an auction closes, a Closing Public Notice is released. This public notice announces winning bidders and long-form application filing deadlines. This public notice also announces the deadlines and procedures for submission of down payments and final payments.

m. Post-Auction Auction Payment Assessments

As appropriate, participants in spectrum auctions may be assessed interim and/or final bid withdrawal payments or default payments.

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Debt Collection	
	Directive Number: FCC INST 1064.4	Effective Date: April 2016

1. **PURPOSE:** This Directive sets forth the policies and procedures of the Federal Communications Commission (“FCC” or “Commission”) pertaining to the collection of non-tax debts owed to the U.S. Government arising out of the activities of or referred to the Commission (including activities of the Commission’s reporting components), including treatment of debt compromise requests and uncollectible debts, and closing out systems and records identifying such debts. Under the law, and for the purpose of this Directive, the terms “claim” and “debt” are synonymous.
2. **AUTHORITY:**
 - a. The Debt Collection Improvement Act (DCIA) of 1996, Pub. L. No. 104-134, 110 Stat. 1321, 1358 (1996) (*codified* at 31 U.S.C. §§ 3701 through 3720E).
 - b. FCC Rules implementing DCIA, 47 C.F.R. Parts 0 (47 C.F.R. §§ 0.11 through 0.392) and 1 (47 C.F.R. §§ 1.1901-1.1953).
 - c. Digital Accountability and Transparency Act of 2014 (Data Act), Pub. L. No. 113-101, 128 Stat. 1153 (2014) (See Sec. 5. Debt Collection Improvement amending 31 U.S.C. § 3716(c)(6)).
 - d. Federal Claims Collection Standards, 31 C.F.R. Parts 900 through 904.
3. **SCOPE:** This directive applies to all Bureaus and Offices of the Commission, and reporting components.
4. **BACKGROUND:** The Debt Collection Improvement Act (DCIA) of 1996, as codified, requires that federal agencies collect debts, assess charges of collection and impose administrative sanctions, transfer delinquent debts to the U.S. Treasury for further collection action or, as appropriate, refer debts to the Department of Justice (DOJ) for enforced collection, and bar delinquent Federal debtors from obtaining Federal loans or guarantees. The Commission’s rules implementing the DCIA parallel the Federal Claims Collections Standards promulgated by DOJ and the Secretary of the Treasury. The Commission’s regulations and changes are consistent with the foregoing DOJ and Treasury authorities.
5. **POLICY:** The Commission will:

- a. Aggressively pursue delinquent debts owed to the Commission (including interagency requests).
- b. Provide delinquent debtors required due process (as set forth at 47 C.F.R. § 1.1911), to include notification prior to the offsetting any payments to the debtor or referring debts to Treasury's cross-servicing program.
- c. Negotiate, approve, or reject requests for debt compromise (for debts of not more than \$100,000) and/or installment payment of debts in hardship cases.
- d. Accord hearings to debtors, if requested.
- e. Report written off and closed out debts on the Treasury Report on Receivables (TROR).
- f. Except as prohibited by the United States Bankruptcy Code, bar (or "red light") delinquent debtors from receiving Commission benefits and withhold action on applications until the delinquency has been resolved.
- g. Negotiate and accept, as appropriate, installment plans following imposition of a Notice of Apparent Liability (NAL) or Forfeiture Order (FO) (independent from enforcement actions by DOJ) when an initial or partial payment is made.

6. RESPONSIBILITIES:

- a. Pursuant to the Commission's rule at 47 C.F.R. § 0.211, the Chairman is the Head of the Agency or Agency Head for all administrative determinations pursuant to the DCIA. The Chairman is responsible for assuring that the Commission complies with all debt collection requirements applicable to the Commission. The Chairman is required to collect claims of the United States for money or property arising out of activities of the Agency, and has the authority to compromise or suspend or terminate collection on debts not more than \$100,000.
- b. Pursuant to the authority delegated in 47 C.F.R. § 0.231, the Managing Director, under the supervision of the Chairman, is authorized to perform all administrative determinations under the DCIA pertaining to Commission claims (including debt collection, and compromise or suspension and termination of collection of debts not more than \$100,000 and under 47 C.F.R. § 0.11, is responsible for:
 - 1) The creation and management of internal procedures to monitor the Commission's debt collection activities.
 - 2) Ensuring that the Commission's financial management systems comply with all applicable rules and regulations.
- c. The Managing Director has delegated to the Chief Financial Officer (CFO) and the Deputy Chief Financial Officer (DCFO) the authority to perform all administrative determinations under the DCIA pertaining to Commission claims including:
 - 1) Debt collection and compromise, or suspension or termination of collection action

- on debt not more than \$100,000.
 - 2) Monitoring compliance with government policies and directives regarding debt collection.
 - 3) Ensuring compliance with 31 U.S.C. § 3711(g)(1), 31 U.S.C. § 3716(c)(6) and 31 C.F.R. Part 285.12 by transferring to Treasury non-tax debt that is 120-days delinquent.
 - 4) Ensuring compliance with IRS directives and rules concerning compromise or discharge of debt.
 - 5) The creation and management of internal procedures to monitor the Commission's debt collection activities.
- d. The Chief, Financial Operations Revenues & Receivables Operations Group (FO-RROG), is responsible for:
- 1) Maintaining an accounts receivable financial subsystem, which properly records, tracks and posts amounts from inception of the debt through termination.
 - 2) Determining when a debt is delinquent.
 - 3) Ensuring that appropriate debt collection procedures are followed.
 - 4) Issuing Payment Demand Letters (PDL) for delinquent debts.
 - 5) Reviewing and certifying cases prior to referral to FCC Office of General Counsel (OGC), Treasury, Office of Personnel Management (OPM) or to an appropriate credit reporting agency.
 - 6) Reporting on the status of debts.
 - 7) Giving guidance on complicated debt collection action.
 - 8) Providing delinquent debt details and recommendations to the CFO and DCFO concerning the termination of collection action, and the write off and close out of uncollectible debts.
 - 9) Working with Financial Systems Operations Group (FSOG) in providing Bureau/Office access to Financial Operations financial system.
- e. The Commission Bureau/Office Chiefs are responsible for assisting the Managing Director and Chief Financial Officer in carrying out debt collection functions:
- 1) Verifying the validity and amount of delinquent outstanding debt to the CFO/DCFO as of the date of delinquency.
 - 2) Reviewing the Commission's red light list of delinquent nontax debtors upon receipt of an application and prior to the grant or decision on an application.
 - 3) Notifying a delinquent debtor with an application filed of the red light status, including notice as set forth at 47 C.F.R. § 1.1910, and the consequences of failing to pay the delinquent debt.
 - 4) Providing necessary information to the offices of General Counsel and/or Managing Director.
 - 5) Reviewing Section 8 (47 U.S.C. § 158) Application Fee filings to ensure correct fee payment prior to granting of application.
 - 6) Assisting OMD during the annual Section 9 (47 U.S.C. § 159) Regulatory Fee filing process by verifying that the license assessments are correct.
-
- f. Pursuant to 47 C.F.R. §0.251, the Office of General Counsel (OGC) is also authorized to perform all administrative determinations provided by the DCIA.

7. DEMAND FOR PAYMENT AND NOTICES:

- a. Introduction. A claim or debt (the terms are synonymous) means any amount of funds or property that has been determined by an appropriate official of the Federal Government to be owed to the United States by a person, organization, or entity other than another Federal agency (31 U.S.C. § 3701(b)(1)). A debt comes into existence when the Government agency determines that there is a debt, unless some statute provides otherwise. The Government does not have to go to court to establish the indebtedness except in matters that arise from the issuance of an NAL or FO. A negotiated Consent Decree (CD) may result in a contractual agreement to pay a debt, and a default may result in a delinquent debt. The demand to pay the debt by a specific date establishes the date the debt becomes delinquent. Under both statutory and common law the Commission may apply administrative offset, collect interest, and impose administrative charges. The Commission's demand for payment should comply with 47 C.F.R. § 1.1911 to include the appropriate due process notification of the consequences of failing to make prompt and complete payment.
- b. Demand for Payment. No specific form to a demand for payment is required – the Commission may use a letter, order, memorandum, or other form of written communication that provides essential information as set forth below. For control, OMD should make the written demand and/or be informed of an action by a Bureau/Office that incorporates the demand into another document. The written demand for payment should be specific to notify the debtor of the amount and nature of the debt, the due date, and the consequences of failure to pay by the due date. The demand letter must, at a minimum, include:
 - 1) The basis for the debt, and the opportunities to request a Commission review of the indebtedness;
 - 2) The applicable standards for assessing interest, penalties, and charges of collection;
 - 3) The date by which payment is to be made to avoid late charges and enforced collection;
 - 4) The name, address, and telephone number of a Commission point of contact.
 - 5) The Commission's willingness, if applicable, to discuss alternative methods of payment structure;
 - 6) The Red Light Rule sanction of withholding action and dismissal of an application.
 - 7) Other remedies available to the FCC to enforce payment of the debt (including assessment of interest, costs and penalties, administrative offset and litigation), reporting the debtor's delinquency to credit bureaus, the use of private collection agencies, and reporting of the debt to the Internal Revenue Service as discharged, which may result in income tax liability; and.
 - 8) The requirement that nontax delinquent debts may be transferred to the Department of the Treasury for collection at any time, and not later than 120-days from the date of delinquency.

8. MAIL PROCEDURES:

- a. The Demand letter will be forwarded to the debtor via U.S. Postal Service (U.S.P.S.) mail using the FCC's Commission Registration System (CORES) contact address.

- b. Notices and letters sent to debtors will be mailed U.S.P.S. on or before the date printed on the notices and letters. In certain instances, where proof of service is necessary, the correspondence will be sent by U.S.P.S. Certified Mail, Return Receipt Requested, or expedited signature receipt delivery. As provided in any other agreement among the parties, or as may be required by exigent circumstances, the Commission may use other forms of delivery, including facsimile telecopy or electronic mail.

9. RED LIGHT PROCESS:

Under the Commission's Red Light Rule (47 C.F.R. § 1.1910), the Commission will withhold action on and dismiss an application filed by a delinquent debtor. Section 1.1910 provides for a review process of applications and fee payments with the applicant's FCC Registration Number (FRN) to determine whether the applicant is delinquent in paying a debt owed to the Commission or whether the appropriate fee has been paid. The Commission will notify an applicant found to be delinquent that action will be withheld on the application until full payment or an arrangement to pay has been made, and if the debt remains unpaid after 30-days, the application will be dismissed. Withholding and dismissal will not apply if the applicant has filed a timely challenge through an administrative appeal or a juridical proceeding as to the existence or amount of the debt owed the Commission.

The Commission and the reporting entities will provide timely reports of delinquent debtors to the red light system database. B/Os will determine, from a review of the Commission's financial records and the Red Light Display system whether any delinquent debt exists. This review for delinquent debt may be initiated at any time by the B/O, but it must be performed when the application is first received by the Commission and again as close to the actual grant date as possible. An applicant's FCC Registration Number (FRN) will be used to determine all delinquent debt owed attributable to all entities using the same Tax Payer Identification Number (TIN). All Commission electronic systems will be linked and will check the FRN provided on the filing for eligibility-based fee sufficiency and the existence of any non-tax delinquent debt through the FCC financial system. All FRNs provided on the filing are to be checked for delinquent debt and the delinquency of any entity covered by the same TIN will trigger the Red Light. In no case will the application or other request for benefit be granted until the delinquent debt issue has been resolved.

Delinquent debtors will be promptly notified by OMD/FO of all applications held pending Red Light resolution. Notification will be sent to the CORES contact address. OMD/FO will respond to a delinquent debtor's request to pay or arrange to pay delinquent debt. Applications for emergency authorizations and Special Temporary Authority (STA) applications involving safety of life or property, including national security emergencies, will not be subject to the Red Light rule. Further, the exceptions are expanded to include situations where an entity's license is cancelled or expired, and where the entity seeks a STA in order to continue providing service to a substantial number of customers or end-users for a brief period until those customers or end-users can be transitioned to other methods of communications.

As set forth in section 1.1164 and 1.1167, a petition for reconsideration or application for review of a fee determination does not relieve licensees from the requirement to make full and proper payment of the underlying fee and it does not prevent the Commission from dismissing

the petition or application if the underlying debt is delinquent.

10. MANDATORY REFERRAL OF DEBTS TO THE U.S. TREASURY DEPARTMENT:

Any delinquent legally enforceable non-tax debt may be referred to the Treasury for administrative offset and cross servicing before the debt is 120-days delinquent. See 31 C.F.R. § 285.12; 31 C.F.R. § 901.01; 31 C.F.R. § 3716 and 47 C.F.R. § 1.1917. OMD-FO is responsible for ensuring that delinquent debts are transferred to Treasury.

a. The following debts are exceptions to referral:

- 1) Debts that are not legally enforceable;
- 2) Debts under appeal;
- 3) Debts in litigation or foreclosure proceedings;
- 4) Debts of another federal agency;
- 5) Debts which are scheduled for sale under an approved asset sale program;
- 6) Debts which have been referred to a private collection contractor for a period of time acceptable to the Secretary of Treasury;
- 7) Debts which have been referred to Treasury-designated “debt collection centers” for a period of time acceptable to the Secretary of Treasury;
- 8) Debts which will be collected within three (3) years of the date of delinquency through internal offset procedures; and
- 9) Debts exempt by order of the Secretary of the Treasury.

11. REFERRAL OF DEBTS TO THE DEPARTMENT OF JUSTICE FOR LITIGATION AND ENFORCED COLLECTION.

This FCC Office of General Counsel (OGC) option involves DOJ enforcing collection on behalf of the Commission in the courts for those claims that meet the individual DOJ US Attorney Office amount standards, exclusive of interest, penalties, and administrative costs. Referral shall be in accordance with 31 C.F.R. Part 904 and 47 C.F.R. § 1.1917. Specific requirements include OGC preparation of a Claims Collection Litigation Report (CCLR) and the collection and preservation of evidence. See 31 C.F.R. §§ 904.1 – 904.4.


12. INTEREST, PENALTY AND ADMINISTRATIVE FEES:

Interest, penalties, and administrative fees will be charged as provided by 31 U.S.C. 3717 and following the procedures set forth at 31 C.F.R. § 901.2 and 47 C.F.R. § 1.1940. Specifically:

- a. Interest accrues from the date of delinquency, or as otherwise provided by the terms of any contract, note, or security agreement, regulation, or law.
- b. Unless otherwise established in a contract, repayment agreement, or by statute, the rate of interest charged shall be the rate established annually by the Treasury in accordance with 31 U.S.C. 3717. Pursuant to 31 U.S.C. 3717, the Commission may charge a higher rate of interest if it reasonably determines that such a higher rate is necessary to protect the rights of the United States. The Commission should document the reason(s) for its determination that the higher rate is necessary.
- c. Except as provided in a contract, prepayment agreement, or by statute, the rate of interest,

as initially charged, shall remain fixed for the duration of the indebtedness. When a debtor defaults on a repayment agreement and seeks to enter into a new agreement, the agency may require payment of interest at a new rate that reflects the current value of funds to the Treasury at the time the new agreement is executed (or as negotiated in repayment plan). Interest shall not be compounded, that is, interest shall not be charged on interest, penalties, or administrative costs required by this section. If, however, a debtor defaults on a previous repayment agreement, charges that accrued but were not collected under the defaulted agreement shall be added to the principal under the new repayment agreement.

- d. The Commission shall assess administrative costs incurred for processing and handling delinquent debts. The calculation of administrative costs may be based on actual costs incurred or upon estimated costs as determined by the Commission.
- e. Unless otherwise established in a contract, repayment agreement, or by statute, the Commission will charge a penalty, pursuant to 31 U.S.C. 3717(e)(2), not to exceed six percent (6%) a year on the amount due on a debt that is delinquent for more than 90-days. This charge shall accrue from the date of delinquency. If the rate permitted under 31 U.S.C. §§ 3717 is changed, the Commission will apply that rate effective with the change.
- f. The Commission may increase an “administrative debt” by the cost of living adjustment in lieu of charging interest and penalties under this section. “Administrative debt” includes, but is not limited to a debt based on fines, penalties, and overpayments, but does not include a debt based on the extension of Government credit, such as those arising from loans and loan guaranties.



Mark Stephens
Acting Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Ratification of Unauthorized Commitments	
	Directive Number: FCCINST 1073.3	Effective Date: April 15, 2015

1. Purpose. The purpose of this directive is to establish policy, procedures, and responsibilities of the Federal Communications Commission (FCC or Commission) for ratifying unauthorized commitments.
2. Reinstatement. This directive replaces FCC INST 1073.2 (dated September 15, 2011).
3. Scope. All unauthorized commitments are covered by this directive, but the specific circumstances of any particular unauthorized commitment may preclude ratification.
4. Definition. An “unauthorized commitment” is an agreement for goods or services that is not binding solely because the Government representative who made it lacked the authority to enter into the agreement on behalf of the Government. It is sometimes also loosely referred to as an “unauthorized procurement” or “unauthorized contract.”
5. Policy. The Federal Acquisition Regulation (FAR) (48 C.F.R. ch.1) and Standards of Ethical Conduct (5 C.F.R. Part 2635) shall be followed in the conduct of the FCC’s acquisitions and in the management and implementation of its procurement program. Accordingly:
 - a. FCC employees shall not knowingly make unauthorized commitments of any kind, including those that purport to bind the Government in contract. Although the procedures provided in this Directive are for use in those cases where the ratification of an unauthorized commitment is necessary, these procedures must not be used in a manner that facilitates such commitments by FCC employees. Under the FAR, FCC must take positive action to preclude, to the maximum extent possible, the need for ratification actions.
 - b. Only a duly appointed Contracting Officer (with a warrant sufficient to cover the transaction at issue), or a Contracting Officer designated by regulation, is authorized to commit the Commission contractually and sign a contract, purchase order, task order, or delivery order or modify a contract on behalf of the Commission. An exception exists for authorized Government purchase card holders other than Contracting Officers who may use a purchase card to acquire appropriate goods or

services if the FCC's total commitment (including all automatic recurring commitments) is below the micro-purchase threshold. Purchase card transactions are governed by FAR 13.301 and FCC INST 1097.2. Otherwise, employees within the Enterprise Acquisition Center (EAC) are chiefly responsible for day-to-day implementation of the Commission's procurement program. Authorized officials and employees in that function are responsible for the negotiation, execution, administration, and maintenance of the agency's contracts and orders, assisted by representatives from other functions where and to the extent delegated.

- c. No unauthorized commitment of Commission funds shall be honored unless it is ratified in accordance with the procedures set forth in this directive. Any employee that makes an unauthorized commitment that is not subsequently ratified under this Directive or otherwise approved for payment by the Managing Director ***shall be personally responsible for any enforceable obligation to pay the vendor or provider of the goods or services.*** In unusual cases, the Managing Director, after receiving written advice of the Office of General Counsel (OGC), may be able to authorize payment of unauthorized commitments (or what appear to be unauthorized commitments) in full or in part on other, very narrow, legal grounds.
- d. The ratifying official may ratify an unauthorized commitment only when the following conditions exist:
 - (1) Supplies or services have been provided to and accepted by FCC, or FCC otherwise has obtained or will obtain a benefit resulting from performance of the unauthorized commitment;
 - (2) The resulting contract would otherwise have been proper if made by an appropriate Contracting Officer;
 - (3) The Contracting Officer reviewing the unauthorized commitment determines the price to be fair and reasonable;
 - (4) The Contracting Officer recommends payment;
 - (5) Funds are available *and* were available for the goods or services at the time the unauthorized commitment was made;
 - (6) The ratification is in accordance with any limitations prescribed by the FCC under agency procedures applicable to the transaction in issue; and
 - (7) Ratification is in the Commission's interest.

- 6. Ratification Authority. The Senior Procurement Executive (SPE) for EAC is designated as the ratifying official for the Commission.

7. Responsibilities.

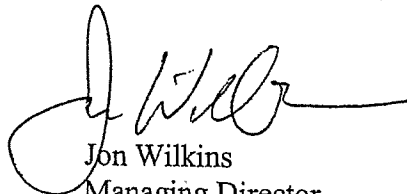
- a. The ratifying official is responsible for:
 - (1) The final decision in all ratification cases;
 - (2) Ensuring compliance with 48 CFR § 1.601-3 and this directive;
 - (3) Developing, implementing, and administering policies and procedures pertaining to unauthorized commitments; and
 - (4) Developing additional procedures based on periodic reviews to preclude future unauthorized commitments.
- b. The Chief Financial Officer shall forward copies of invoices for which no recorded obligation exists to the Chief, EAC, except invoices for travel which shall be forwarded to the appropriate bureau or office chief (see paragraph nine).
- c. The Chief, EAC shall:
 - (1) Be responsible for assembly of the ratification file as set forth in paragraph eight; and
 - (2) Recommend to the ratifying official whether to ratify an unauthorized commitment based on consideration of the criteria in paragraph 5.d.
- d. Bureau and Office Chiefs shall ensure that:
 - (1) Employees under their supervision provide to the Contracting Officer upon request all pertinent data concerning the unauthorized commitment;
 - (2) Employees under their supervision comply with the FAR 48 C.F.R. § 1.601-3 and this directive;
 - (3) Precautionary measures to reduce and prevent unauthorized commitments, as prescribed by the Managing Director or designee, are taken within their respective bureaus and offices; and
 - (4) Supervisory staff advise employees of the Commission's policies regarding unauthorized commitments.

8. Ratification Procedure.

- a. The EAC shall assemble the ratification file. For cases involving more than \$500, the file, at a minimum, shall contain the following:
 - (1) A statement from the Commission employee who made the unauthorized commitment explaining the facts and circumstances of the matter;
 - (2) A summary statement of the facts of the unauthorized commitment from the Chief, EAC to the ratifying official, along with a recommendation on action to be taken addressing each of the conditions and areas for recommendation or determination identified in paragraph 5.d. above; and
 - (3) A statement whether the official or employee responsible for the unauthorized commitment has previously made unauthorized commitments, including their number, value, and nature.
- b. In cases involving \$500 or less, a summary ratification procedure may be used. Under the summary procedure, the file shall take the form of a memorandum sent by the Chief, EAC to ratifying official. The memorandum shall describe the circumstances necessitating the summary ratification, address each of the conditions and areas for recommendation or determination identified in paragraph 5.d. above, recommend an action, and provide an approval/disapproval line for the ratifying official's signature. This signed memorandum shall be the authorizing document for the payment of the obligation.
- c. Prior to forwarding the recommendation on a case involving more than \$500 to the ratifying official, OGC shall review the recommended action. OGC may concur with the recommendation for payment or return it to the Chief, EAC with a rationale for non-concurrence. The ratifying official may act favorably upon a recommendation for payment without the concurrence of legal counsel in any case involving \$500 or less, or, in the ratifying official's sole discretion, for exigent or compelling circumstances with respect to cases involving more than \$500.
- d. After reviewing the file, the ratifying official shall decide whether to ratify the unauthorized commitment, sign the appropriate documents, and return the file to the EAC for disposition. The ratifying official may recommend disciplinary action for resolution by the appropriate supervisor or office chief, if any, and if the determination is not to ratify the unauthorized commitment, shall determine, in consultation with OGC, the appropriate action to be taken to resolve the matter.

9. Quarterly Reporting Requirements.

- a. The ratifying official shall provide a report to the MD and SMC for review at their quarterly meetings summarizing the number of ratifications processed for the prior quarter. The report, at a minimum, shall contain the following:
 - (1) The number of ratification actions processed, including the dollar amounts and the office responsible for each unauthorized commitment;
 - (2) A listing of outstanding ratifications and any actions needed to complete the process;
 - (3) A listing of any unauthorized commitments that were not approved for ratification, and a description of those actions to include a description of the risks to the Commission, if any, and other possible remedies for such items to include input from OGC.
- b. The ratifying official shall include a scorecard within the ratification report provided to the MD and the SMC for review at their quarterly meetings. The scorecard shall contain the following measures:
 - (1) Low Risk - Actions Completed. For completed ratifications, with no outstanding issues, the scorecard shall include the number of actions by quarter and for the current and most recent fiscal year.
 - (2) Medium Risk - Actions Under Process. For unauthorized commitments under process, without significant completion issues, the scorecard shall include the number of actions by quarter and for the most recent fiscal year.
 - (3) High Risk – Actions Not Approved. For unauthorized commitments not approved, or at risk of disapproval, the scorecard shall include the number of actions by quarter and for the most recent fiscal year, plus detailed notes that include input from OGC, that address the specific risks to the commission, and all other relevant issues.



Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Interagency Agreements	
	Directive Number: FCCINST 1074.1	Effective Date: August 2016

1. **PURPOSE.** This document provides guidance to Federal Communications Commission's (FCC or Commission) Bureaus/Offices (B/O) on the procedures for entering into Interagency Agreements (IAAs) with other Federal agencies that involve the transfer of funds between or among Federal agencies to provide, obtain, or share services, goods, or rights.
2. **SCOPE.** This directive applies to headquarters and field units. The directive does not apply to:
 - A. Agreements between or among agencies on matters of common interest that do not involve the transfer of funds.
 - B. The detail of personnel between agencies (although such details may sometimes require compliance with the Economy Act).
 - C. "Direct acquisitions," as that term is defined and construed in section 2.101 and Subpart 17.5 of the Federal Acquisition Regulation (although such actions may involve detailed requirements for FCC's direct use of third-party agency contract vehicles, including the need for a delegation of authority or other procedural requirements).
3. **AUTHORITIES.** Each IAA must identify the statutory authority for the transfer of funds from the requesting agency to the servicing agency for the services and/or supplies to be provided. We list below frequently used authorities for the transfer of funds under an IAA. The list is instructive but not exhaustive.
 - A. The Economy Act, 5 U.S.C. § 1535. This is the most commonly used authority for the transfer of funds. If, however, either agency has a more specific statutory authority that covers the particular transfer of funds for the IAA, that more specific authority *must* be used instead of the Economy Act;

- B. The General Services Administration Modernization Act, 40 U.S.C. § 321, which provides authority for the Acquisition Services Fund (previously known as the General Services Information Technology Fund);
- C. The Government Management Reform Act of 1994, 31 U.S.C. § 501 note, which establishes the franchise funds, such as GovWorks (Department of Interior) and FedSource (Department of the Treasury);
- D. The Government Employees Training Act, 5 U.S.C. § 4104; and
- E. The Office of Personnel Management Revolving Fund, 5 U.S.C. § 1304(e)(1).

If it is unclear what statutory authority should be relied on for a particular IAA, B/Os should consult the Senior Procurement Executive (SPE).

4. DEFINITIONS.

- A. Assisted Acquisition(s): Interagency acquisitions for which a Requesting Agency, at its discretion, has determined that it is in the best interest of the government to seek the acquisition services of a Servicing Agency in the procurement of supplies or services from the private sector (or from an Federal Funded Research and Development Center (FFRDC) that does not accept direct orders) and where the Servicing Agency awards a contract or order on behalf of the Requesting Agency.
- B. Direct Acquisition: means a type of interagency acquisition where a requesting agency places an order directly against a servicing agency's indefinite-delivery contract. The servicing agency manages the indefinite-delivery contract but does not participate in the placement or administration of an order.
- C. Interagency Agreement: A written agreement between Federal agencies or Components of Federal agencies to acquire supplies or services as authorized by statute.
- D. Interagency Acquisition: A procedure by which an agency needing supplies or services (the requesting agency) obtains them from another agency (the servicing agency), by an assisted acquisition or a direct acquisition.
- E. Requesting Agency: A Federal agency that has a requirement and desires to obtain goods or services from a Servicing Agency.
- F. Servicing Agency: A Federal agency that is willing and able to provide goods or services to a Requesting Agency.

- 5. POLICY. It is the policy of the FCC that an IAA with other Federal agencies will only be entered into when it is legally permissible.

- A. IAAs must be prepared and administered in accordance with this directive. The B/O Assistant Bureau Chief (ABC) must obtain initial approval for an IAA from the Chief Financial Officer (CFO). Once that approval is obtained, the B/O must submit the draft IAA to the Budget Center for review.
- B. All IAAs must be approved by the SPE prior to being presented to the Managing Director or his/her designee for signature.
- C. An IAA signed by officials at both agencies must be in place before commencement of services and/or provision of supplies under the IAA. Similarly, an IAA signed by officials at both agencies must be in place before any funds transfer can be made.
- D. If the IAA involves an assisted acquisition (*i.e.*, where another agency will be performing acquisition activities on behalf of the FCC, such as awarding a contract or placing on order, or vice versa), then certain procurement requirements are triggered, which will be fulfilled by a contracting officer in the Enterprise Acquisition Center (EAC), who will be supported by one or more representatives of the B/O with the requirement.

6. RESPONSIBILITIES.

- A. Managing Director. Approves all IAAs between the FCC and other Federal agencies involving the transfer of funds between agencies to provide goods or services.
- B. Senior Procurement Executive:
 - (1) Reviews all proposed IAAs and recommends action to the Managing Director.
 - (2) Serves as the FCC's subject matter expert on IAAs, responding to questions posed by Bureau/Office staff and management.
 - (3) Ensures that all requirements of the FAR are met for interagency acquisitions, especially the assisted acquisitions that require IAAs.
- C. Chief Financial Officer:
 - (1) Initially considers all requests for IAAs proposed by program offices.
 - (2) Reviews completed IAA packages to ensure fund availability as well as accuracy of accounting and financial data.
- D. General Counsel:
 - (1) Provides advice to OMD and/or SPE on legal questions relating to authority to enter into an IAA.
 - (2) Provides advice to OMD and/or SPE on legal questions relating to proposed terms of an IAA.
 - (3) Provides advice to OMD and/or SPE in the event of a legal dispute between the agencies regarding the terms of an IAA.

- (4) Provides advice to OMD and/or SPE on legal questions relating to compliance with FAR Subpart 17.5 (Interagency Acquisitions).

E. Bureaus/Offices:

- (1) Proposes IAAs that will be beneficial in fulfilling the mission of the FCC.
- (2) Drafts the IAA and proposed Statement of Work, with the assistance, where necessary of EAC.
- (3) Collaborates and supports EAC in its preparation and execution of a determination of best procurement approach, written agreement on responsibility for management and administration of solicitations, contracts, and orders arising from assisted acquisitions; and other determinations and finding required by the FAR. *See* 7.J. and L. (below).
- (4) Once approved, monitors the provision of goods and/or services obtained under the IAA to ensure the FCC receives full value and that the terms and conditions of the IAA are fulfilled.

7. GENERAL PROCEDURES.

A. Program officials are to submit requests for IAAs to their Assistant Bureau Chief for Management (or Deputy Bureau Chief as an alternative), who will request initial approval from the CFO or his/her designee. If the CFO or his/her designee approves the request for an IAA, the program office shall initiate the IAA process by completing the following steps and forwarding the draft documents to the Budget Center:

- (1) Draft the IAA. To the maximum extent possible, IAAs shall be prepared using the current version of Department of Treasury's FMS Form 7600, which consists of two sections: (i) General Terms and Conditions (Form 7600A) and (ii) Order which obligates funds (Form 7600B);
- (2) Enter the accounting information into Genesis; and
- (3) Provide a Statement of Work (SOW), if the FCC contemplates an assisted acquisition by a servicing agency or requires a statement of work for direction of work to be performed by the servicing's agency's own employees.

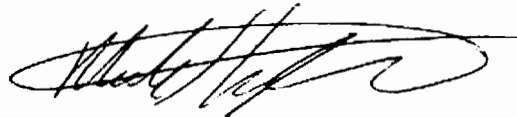
B. The Budget Center reviews all forms and the SOW (if applicable) and completes the following actions:

- (1) Reviews for accuracy all accounting information provided in the required forms;
- (2) Certifies fund availability for the IAA;
- (3) Ensures all financial codes are accurately provided on the FMS Form 7600B;
- (4) Assigns the IAA number (if the FCC is the requesting agency);
- (5) Create the External Direct Agreement (ERA) for IAAs, in which the Commission is the servicing agency; and

- (6) The Budget Center forwards the completed IAA package to the SPE for review.
- C. If an assisted acquisition is contemplated, EAC has final responsibility for compliance with the requirements of the FAR Subpart 17.5, and the B/O with the requirement is expected to provide its complete cooperation and support to EAC to enable EAC to discharge this responsibility.
- D. The SPE may consult with OGC on any legal questions concerning appropriate statutory authority for the IAA and/or interpretation of provisions of the IAA.
- E. Only the Managing Director or his/her designee is authorized to execute Form 7600A. Only the Chief Financial Officer (CFO) or his/her designee is authorized to execute Form 7600B as a funding official, which obligates funds. For IAA's involving assisted acquisitions, Form 7600B (Block 40) must be completed with the contact information for the contracting officer responsible for FCC's procurement responsibilities as requesting or servicing agency, and signed and dated. In the event that another agency insists on using its own IAA form or a Memorandum of Agreement (MOA), only the Managing Director or his/her designee is authorized to execute the document.
- F. If the FCC is the requesting agency, once the IAA is executed by both agencies, the SPE shall send the executed IAA to the Budget Center for entry into the Financial Management System (Genesis) so that the funds can be obligated.
- G. EAC shall maintain the official copies of all IAAs once they are executed and monitor the performance of all IAAs once they are in place.
- H. Economy Act Documentation Requirement. If authority to transfer funds under the IAA is pursuant to the Economy Act, specific documentation (a determination and finding (D&F)) must be executed prior to signing of the IAA. If the FCC is the servicing agency, the D&F is the responsibility of the requesting agency. If the FCC is the requesting agency, the D&F shall be prepared and executed by the program office (unless the IAA involves an assisted acquisition, in which case the document must adhere to the requirements in Federal Acquisition Regulation (FAR) 17.502-2(c) and be executed by a contracting officer in EAC). The supporting D&F shall state that the following requirements of 31 U.S.C. § 1535(a) have been met:
- (1) Funds are available in the amount required for the IAA;
 - (2) The IAA is in the best interest of the Federal Government;
 - (3) The servicing agency is able to provide the required goods or services; and
 - (4) The required goods or services cannot be provided by contract as conveniently or cheaply by a commercial enterprise.
- I. Duration of IAAs. An IAA must specify a period of effectiveness. An IAA is usually effective from the date that it is signed by the Managing Director or

his/her designee and remains in effect for the period specified in the IAA unless modified or terminated. B/Os shall monitor the end date of existing IAAs and ensure that new IAAs are prepared and submitted for review in a timely manner to ensure there is no lapse of service. An IAA may include provisions for IAA renewal on an annual basis. If the proposed term of an IAA will exceed one year, consult the SPE.

- J. Assisted Acquisitions. If the IAA provides for the servicing agency to perform an assisted acquisition on behalf of the FCC, EAC shall prepare and execute a Determination of Best Procurement Approach in accordance with FAR 17.502-1(a)(1). EAC and the program office will work together to prepare and negotiate with the servicing agency (as part of the Form 7600B or an incorporated attachment) a written agreement on responsibility and management of the acquisition in accordance with FAR 17.502-1(b). Alternatively, where a series of orders are contemplated that will involve several assisted acquisitions that can be addressed by a uniform approach on responsibility and management for the acquisitions, the agreement on responsibility and management of the acquisition can be made or reflected in the Form 7600A. If the assisted acquisition is being conducted under the authority of the Economy Act, a D&F is required in accordance with FAR 17.502-2(c). If the FCC is the requesting agency, the D&F is initiated by the program office, with assistance from EAC if necessary, and executed by a contracting officer in EAC. If the FCC is the servicing agency, EAC shall ensure that a copy of an executed D&F has been provided by the requesting agency.
- K. Modifications of IAAs and Orders. If an IAA or order needs to be modified, the program office shall prepare the modifications on the appropriate form and submit the form to the Budget Center. After review, the Budget Center shall send the form to the SPE for processing and approval. Modifications to IAAs must be executed by the Managing Director or his/her designee; modifications to orders must be executed by the CFO or his/her designee.



Mark Stephens
Managing Director

United States Government
Interagency Agreement (IAA) – Agreement Between Federal Agencies
General Terms and Conditions (GT&C) Section

IAA Number _____ - 0000 - _____
GT&C # _____ Order # _____ Amendment/Mod # _____

DEPARTMENT AND/OR AGENCY		
1.	Requesting Agency of Products/Services	Servicing Agency Providing Products/Services
Name		
Address		
2. Servicing Agency Agreement Tracking Number (Optional) _____		
3. Assisted Acquisition Agreement Yes <input type="checkbox"/> No <input type="checkbox"/>		
4. GT&C Action (Check action being taken) <input type="checkbox"/> New <input type="checkbox"/> Amendment – Complete only the GT&C blocks being changed and explain the changes being made. <input type="checkbox"/> Cancellation – Provide a brief explanation for the IAA cancellation and complete the effective End Date.		
5. Agreement Period Start Date _____ End Date _____ of IAA or effective cancellation date <div style="display: flex; justify-content: space-around; width: 100%;"> MM-DD-YYYY MM-DD-YYYY </div>		
6. Recurring Agreement (Check One) A Recurring Agreement will continue, unless a notice to discontinue is received. Yes <input type="checkbox"/> If Yes, is this an: Annual Renewal <input type="checkbox"/> <div style="display: flex; justify-content: space-between; width: 100%;"> Other Renewal <input type="checkbox"/> State the other renewal period: _____ </div> No <input type="checkbox"/>		
7. Agreement Type (Check One) <input type="checkbox"/> Single Order IAA <input type="checkbox"/> Multiple Order IAA		
8. Are Advance Payments Allowed for this IAA (Check One) <input type="checkbox"/> Yes <input type="checkbox"/> No If Yes is checked, enter Requesting Agency's Statutory Authority Title and Citation <div style="height: 100px; border: 1px solid black;"></div>		
Note: Specific advance amounts will be captured on each related Order.		

United States Government
Interagency Agreement (IAA) – Agreement Between Federal Agencies
General Terms and Conditions (GT&C) Section

IAA Number _____ - 0000 -
 GT&C # Order # Amendment/Mod #

9. Estimated Agreement Amount (The Servicing Agency completes all information for the estimated agreement amount.)
(Optional for Assisted Acquisitions)

Direct Cost _____
Overhead Fees & Charges _____
Total Estimated Amount _____ **\$0.00**

Provide a general explanation of the Overhead Fees & Charges

10. STATUTORY AUTHORITY

a. Requesting Agency's Authority (Check One)

Franchise Fund	Revolving Fund	Working Capital Fund	Economy Act (31 U.S.C. 1535/FAR 17.5)	Other Authority
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fill in Statutory Authority Title and Citation for Franchise Fund, Revolving Fund, Working Capital Fund, or Other Authority

b. Servicing Agency's Authority (Check One)

Franchise Fund	Revolving Fund	Working Capital Fund	Economy Act (31 U.S.C. 1535/FAR 17.5)	Other Authority
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fill in Statutory Authority Title and Citation for Franchise Fund, Revolving Fund, Working Capital Fund, or Other Authority

11. Requesting Agency's Scope (State and/or list attachments that support Requesting Agency's Scope.)

12. Roles & Responsibilities for the Requesting Agency and Servicing Agency (State and/or list attachments for the roles and responsibilities for the Requesting Agency and the Servicing Agency.)

United States Government
Interagency Agreement (IAA) – Agreement Between Federal Agencies
General Terms and Conditions (GT&C) Section

IAA Number _____ - 0000 - _____
GT&C # Order # Amendment/Mod #

13. Restrictions (Optional) (State and/or attach unique requirements and/or mission specific restrictions specific to this IAA).

14. Assisted Acquisition Small Business Credit Clause (The Servicing Agency will allocate the socio-economic credit to the Requesting Agency for any contract actions it has executed on behalf of the Requesting Agency.)

15. Disputes: Disputes related to this IAA shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, *Intragovernmental Business Rules* Bulletin, available on the TFM Web site at <http://www.fms.treas.gov/tfm/vol1/bull.html>.

16. Termination (Insert the number of days that this IAA may be terminated by written notice by either the Requesting or Servicing Agency.)

If this agreement is canceled, any implementing contract/order may also be canceled. If the IAA is terminated, the agencies shall agree to the terms of the termination, including costs attributable to each party and the disposition of awarded and pending actions.

If the Servicing Agency incurs costs due to the Requesting Agency's failure to give the requisite notice of its intent to terminate the IAA, the Requesting Agency shall pay any actual costs incurred by the Servicing Agency as a result of the delay in notification, provided such costs are directly attributable to the failure to give notice.

17. Assisted Acquisition Agreements – Requesting Agency's Organizations Authorized To Request Acquisition Assistance for this IAA. (State or attach a list of Requesting Agency's organizations authorized to request acquisition assistance for this IAA.)

18. Assisted Acquisition Agreements – Servicing Agency's Organizations authorized to Provide Acquisition Assistance for this IAA. (State or attach a list of Servicing Agency's organizations authorized to provide acquisition for this IAA.)

19. Requesting Agency Clause(s) (Optional) (State and/or attach any additional Requesting Agency clauses.)

United States Government
Interagency Agreement (IAA) – Agreement Between Federal Agencies
General Terms and Conditions (GT&C) Section

IAA Number _____ - 0000 - _____
GT&C # Order # Amendment/Mod #

20. Servicing Agency Clause(s) (Optional) (State and/or attach any additional Servicing Agency clauses.)

21. Additional Requesting Agency and/or Servicing Agency Attachments (Optional) (State and/or attach any additional Requesting Agency and/or Servicing Agency attachments.)

22. Annual Review of IAA

By signing this agreement, the parties agree to annually review the IAA if the agreement period exceeds one year. Appropriate changes will be made by amendment to the GT&C and/or modification to any affected Order(s).

AGENCY OFFICIAL

The Agency Official is the highest level accepting authority or official as designated by the Requesting Agency and Servicing Agency to sign this agreement. Each Agency Official must ensure that the general terms and conditions are properly defined, including the stated statutory authorities, and, that the scope of work can be fulfilled per the agreement.

The Agreement Period Start Date (Block 5) must be the same as or later than the signature dates.

Actual work for this IAA may NOT begin until an Order has been signed by the appropriate individuals, as stated in the Instructions for Blocks 37 and 38.

23.	Requesting Agency	Servicing Agency
Name		
Title		
Telephone Number(s)		
Fax Number		
Email Address		
SIGNATURE		
Approval Date		

United States Government
Interagency Agreement (IAA) – Agreement Between Federal Agencies
Order Requirements and Funding Information (Order) Section

IAA Number _____ - _____ - _____
 GT&C # Order # Amendment/Mod #

Servicing Agency's Agreement
 Tracking Number (Optional) _____

PRIMARY ORGANIZATION/OFFICE INFORMATION

24.	Requesting Agency	Servicing Agency
Primary Organization/Office Name		
Responsible Organization/Office Address		

ORDER/REQUIREMENTS INFORMATION

25. Order Action (Check One)

☐ **New**

☐ **Modification (Mod)** – List affected Order blocks being changed and explain the changes being made. For Example: for a performance period mod, state new performance period for this Order in Block 27. **Fill out the Funding Modification Summary by Line (Block 26)** if the mod involves adding, deleting or changing **Funding for an Order Line**.

☐ **Cancellation** – Provide a brief explanation for Order cancellation and fill in the Performance Period End Date for the effective cancellation date.

26. Funding Modification Summary by Line	Line # _____	Line # _____	Line # _____	Total of All Other Lines (attach funding details)	Total
Original Line Funding	\$	\$	\$	\$	\$ 0.00
Cumulative Funding Changes From Prior Mods [addition (+) or reduction (-)]	\$	\$	\$	\$	\$ 0.00
Funding Change for This Mod	\$	\$	\$	\$	\$ 0.00
TOTAL Modified Obligation	\$ 0.00	\$ 0.00	\$ 0.00	\$ 0.00	\$ 0.00
Total Advance Amount (-)	\$	\$	\$	\$	\$ 0.00
Net Modified Amount Due	\$ 0.00	\$ 0.00	\$ 0.00	\$ 0.00	\$ 0.00

27. Performance Period

Start Date

MM-DD-YYYY

End Date

MM-DD-YYYY

For a performance period mod, insert the start and end dates that reflect the new performance period.

IAA Number _____ - _____ - _____ Servicing Agency's Agreement
 GT&C # Order # Amendment/Mod # Tracking Number (Optional) _____

FMS Form 7600B
07/10

IAA Number _____ - _____ - _____ Servicing Agency's Agreement
GT&C # Order # Amendment/Mod #
Tracking Number (Optional) _____

DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
Page 3 of 5

United States Government
Interagency Agreement (IAA) – Agreement Between Federal Agencies
Order Requirements and Funding Information (Order) Section

IAA Number _____ - _____ - _____ Servicing Agency's Agreement
 GT&C # Order # Amendment/Mod # Tracking Number (Optional) _____

35. Funding Clauses/Instructions (Optional) (State and/or list funding clauses/instructions.)

36. Delivery/Shipping Information for Products (Optional)

Agency Name	
Point of Contact (POC) Name & Title	
POC Email Address	
Delivery Address /Room Number	
POC Telephone Number	
Special Shipping Information	

APPROVALS AND CONTACT INFORMATION

37. PROGRAM OFFICIALS

The Program Officials, as identified by the Requesting Agency and Servicing Agency, must ensure that the scope of work is properly defined and can be fulfilled for this Order. The Program Official may or may not be the Contracting Officer depending on each agency's IAA business process.

	Requesting Agency	Servicing Agency
Name		
Title		
Telephone Number		
Fax Number		
Email Address		
SIGNATURE		
Date Signed		

38. FUNDING OFFICIALS - The Funds Approving Officials, as identified by the Requesting Agency and Servicing Agency, certify that the funds are accurately cited and can be properly accounted for per the purposes set forth in the Order. The Requesting Agency Funding Official signs to obligate funds. The Servicing Agency Funding Official signs to start the work, and to bill, collect, and properly account for funds from the Requesting Agency, in accordance with the agreement.

	Requesting Agency	Servicing Agency
Name		
Title		
Telephone Number		
Fax Number		
Email Address		
SIGNATURE		
Date Signed		

IAA Number _____ - _____ - _____ Servicing Agency's Agreement
 GT&C # Order # Amendment/Mod # Tracking Number (Optional) _____

FINANCE OFFICE Points of Contact (POCs)

39.	Requesting Agency (Payment Office)	Servicing Agency (Billing Office)
Name		
Title		
Office Address		
Telephone Number		
Fax Number		
Email Address		
Signature & Date (Optional)		

This may include CONTRACTING Office Points of Contact (POCs).

DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
Page 5 of 5

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Use of Federal Government Purchase Card for Small Purchases	
	Directive Number: FCCINST 1097.2	Effective Date: April 13, 2015

1. **PURPOSE:** This directive establishes the policy for use of the Federal Communications Commission's ("FCC" or "Commission") Government Purchase Card. The purpose of this directive is to ensure that applicable Federal laws, statutes, and regulations pertaining to the use of Government Purchase Cards are properly adhered to, and to establish agency-specific policies and procedures pertaining to procurement activities.
2. **CANCELLATION:** This instruction replaces FCCINST 1097.1, dated October 2008.
3. **AUTHORITY:**
 - a. 5 U.S.C. § 301. Departmental Regulations.
 - b. Executive Order 12352, "Federal Procurement Reforms."
 - c. Federal Acquisition Regulation (FAR), 48 C.F.R. Chapter 1 (Parts 1 to 51).
 - d. Anti-Deficiency Act (31 U.S.C. §§ 1341, 1342, 1512).
 - e. OMB Circular A-123, Appendices A & B.
4. **SCOPE:** This directive applies to all Bureaus and Offices within the FCC that require purchase card procurement actions to be processed by the Commission.
5. **DEFINITIONS:**
 - a. **Abuse:** Use of a government purchase card to buy authorized supplies or services at terms (e.g., price, quantity) that are excessive or for a questionable government need, or both. Examples: Purchase of a \$300 day planner rather than one that costs \$45; bulk or year-end purchases that are of a questionable government need.
 - b. **Agency Program Coordinator (APC):** The APC serves as the agency's charge card manager and is responsible for implementation and oversight of the FCC's Purchase Card Program.
 - c. **Anti-Deficiency Act:** Making or authorizing an expenditure from, or creating or authorizing an obligation under, any appropriation or fund in excess of the amount available in the appropriation or fund, unless authorized by law.
 - d. **Approving Official (AO):** An individual with oversight and approval responsibility for the

purchase card activities of a limited number of cardholders under his or her purview.

- e. Billing Cycle: A recurring monthly time period for which Statements of Account (SOAs) are processed. The billing cycle for FCC purchase cards begins on the 10th day of each month and ends on the 9th day of the following month.
- f. Billing Cycle Purchase Limit: The spending limit imposed on a cardholder's cumulative purchase card transactions in a given billing cycle.
- g. Cardholder: The individual government employee to whom a government purchase card is issued to purchase goods and services and/or pay for official expenses in compliance with applicable regulations.
- h. Contracting Officer (CO): A Contracting Officer who holds a government purchase card may award contracts that accept the purchase card as the method of payment when payment by purchase card is in the best interest of the government.
- i. Fraud: Any felonious act of corruption or attempt to cheat the government or corrupt the government's agents. For the purposes of this directive, use of government charge cards to transact business that is not sanctioned, not authorized, not in one's official government capacity, not for the purpose for which the card was issued, or not as a part of official government business, are instances of fraud. This definition is not intended to be all inclusive.
- j. GSA SmartPay®: The Federal Government's charge card program. It provides federal agency cardholders with a means to pay for commercial goods and services, travel and travel related expenses, and fleet vehicle expenses. Charge cards are issued through contracts with charge card banks that are a part of the SmartPay® program. These contracts, collectively referred to as the "Master Contract," are administered by the General Services Administration (GSA).
- k. Improper Purchase: Any purchase that should not have been made or that was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements. Incorrect amounts include overcharges and undercharges. An improper purchase can be one of two types: unauthorized or incorrect.
 - Unauthorized purchase: Use of a charge card for other than the official government purpose(s) for which it is intended.
 - Incorrect purchase: A mistake that is the result of an unintentional error during the purchase process. For example, when a cardholder is asked to buy one filing cabinet but purchases three cabinets, this is an incorrect purchase. A series of seemingly incorrect purchases may require investigation to determine whether these purchases are actually unauthorized purchases.
- l. Merchant Category Code (MCC): A four-digit number assigned to a business by MasterCard or VISA when the merchant first starts accepting one of the cards as a form of payment. The MCC is used to classify the business by the type of goods or services it provides.
- m. Micro-Purchase: An acquisition of supplies and services using simplified acquisition procedures to ensure the aggregate amount does not exceed the micro-purchase threshold set by the FAR, which is currently \$3,000 for supplies and \$2,500 for services.

- n. Purchase Card: A bank-issued plastic card, similar to a personal credit card, which authorizes a cardholder to purchase goods or services for official government use. The card is specifically designed showing the United States of America seal and imprinted with the words “For Official U.S. Government Purchases Only” to avoid being mistaken for a personal credit card. The card is also imprinted with “U.S. Government Tax Exempt.”
- o. Purchase Card Log: A manual or automated log in which cardholders document their individual transactions when using their purchase card. Entries in the purchase log may be supported by internal agency documentation; e.g., written requests for procurement, forms, email correspondence, etc.
- p. Reconciliation: The process by which the cardholder and the AO review the monthly Statements of Account, reconcile transactions against merchant receipts and purchase card logs/files, and authorize payment of those charges.
- q. Requirement: The description of the customer’s needs that leads to an acquisition.
- r. Separation of Duties: A mandatory management control to prevent key functions from being performed by the same person. Duties, such as making purchases, authorizing payments, certifying funding and reviewing/auditing will be assigned to different individuals to the greatest extent possible, in order to minimize the risk of loss to the government.
- s. Split Purchase: An improper “split” of a purchase requirement generally involves the willful reduction of a requirement which could be purchased from the same merchant in an effort to keep the total price of the purchase at or below the cardholder’s single purchase limit. Splitting the requirement into individual purchases is improper unless no one merchant has the capability to satisfy the full requirement. A split purchase is a violation of FAR Part 13.003(c) and could result in suspension of a cardholder account. Examples of Split Purchases or Split Requirements include:
- A single cardholder making multiple purchases from the same merchant on the same day, the total of which exceeds the single purchase limit and the total requirement was known at the time of the first purchase.
 - A single cardholder purchasing the same/similar item(s) from multiple merchants on the same day, the total of which exceeds the single purchase limit and the total was known at the time of the first purchase. If the requirement exceeds the cardholder’s single purchase limit, the cardholder cannot buy the items with their purchase card and must forward the requirement to the FCC’s Enterprise Acquisition Center (EAC).
- t. Statement of Account (SOA): Also known as a billing statement. A monthly SOA is received by the cardholder from the purchase card contractor bank showing purchases, payments and credits for the billing period.
- u. Suspension: The process in which a cardholder is prohibited from making purchases with their purchase card. Cards may be suspended as a result of fraudulent purchases, unauthorized use of the card, failure to complete mandatory training, failure to comply with appropriate purchase card procedures or to comply with an audit/review of a card transaction.

- v. Tax Exemption: Government purchase card purchases are exempt from state and local taxes in accordance with the legal incidence of the tax. Tax exemption letters for most states under the GSA Smart Pay program are at <https://smartpay.gsa.gov/about-gsa-smartpay/tax-information/state-response-letter>.

6. PURCHASE CARD SERVICES:

- a. Purchase card services are made available to the FCC by its purchase card contractor bank. The bank issues cards to individual employees appointed as cardholders through FCC procedures; provides cardholders with customer assistance; issues monthly SOAs to cardholders; and assists the APC with program administration tools.
- b. All purchase cards issued to employees shall be authorized by their appropriate Bureau/Office Chief, or their designee. Purchase cards are similar in use to personal credit cards but have controls in place to ensure that purchases are for authorized goods/services and that purchases do not exceed approved dollar thresholds.

7. POLICY:

The following points are FCC policy. All forms referenced in this document may be found at <http://intranet.fcc.gov/omd/hrm/fccforms.html>:

- a. The purchase card shall be used in preference to other methods of procurement for the acquisition of supplies and services that do not exceed the micro-purchase threshold.
- b. The purchase card may not be used to award contracts in excess of the micro-purchase threshold. The purchase card may only be used to place an order in excess of the micro-purchase threshold against an existing contract or agreement when expressly permitted by the contract or agreement. However, an order that exceeds the micro-purchase threshold may be placed only by a cardholder who has a contracting officer's warrant, and the amount of the order may not exceed the maximum amount authorized by the contracting officer's warrant.
- c. A cardholder may not have a single purchase limit in excess of the micro-purchase threshold unless he/she has a contracting officer's warrant. Subject to this limitation, in unusual and exigent circumstances, a cardholder's purchase limit may be increased by the APC upon written request of the cardholder's AO, in order to obtain either a specific item or service for a specific length of time. The circumstances for the purchase limit increase, such as project description, the temporary purchase limit amount, the request from the cardholder's AO, the length of time for which the limit is increased, etc., shall be recorded and retained by the APC.
- d. No requisition or purchase request shall be required from the Bureaus/Offices for card purchases unless the purchase is made by the FCC's Enterprise Acquisition Center (EAC) on behalf of a Bureau/Office, or the purchase is of an unusual nature from a vendor that does not have an acceptable MCC.
- e. Cardholders shall purchase from required purchase sources in accordance with the Federal Acquisition Regulation (FAR) Part 8 and shall purchase from small businesses to the extent practicable.
- f. Purchase card nominees and AO nominees must complete and sign the *FCC Form A-498 Purchase Card Program Application for Cardholder and/or Approving Official* prior to issuance of the purchase card or certification as an AO.

- g. Purchase card nominees and AO nominees must complete the GSA Purchase Card web-based training prior to issuance of the purchase card or certification as an AO. Certificates of Completion of the training must be submitted to the APC prior to issuance of the purchase card. All cardholders and AOs are required to take GSA web-based training as refresher training every three years or as directed by the agency's lead APC, and to provide certification of training to the APC. All cardholders and AOs will adhere to the agency's anti-fraud training requirements set forth in FCC Directive FCCINST 1102.5 "Policy for Detecting and Deterring Fraud and Promoting Ethical Conduct within the Federal Communications Commission."
- h. Cardholders shall reconcile their monthly SOA received from the contractor bank within five (5) workdays after the end of the billing cycle. Upon reconciling the SOA, the cardholder must affix his/her dated signature and printed name on the reconciled SOA and forward it to his/her AO for review.
- i. AOs shall review each reconciled SOA received from their purchase cardholders within seven (7) workdays after the end of the billing cycle. Upon review, the AO must affix his/her dated signature and printed name on the reconciled SOA. The AO then must forward the reconciled SOA to the Office of Financial Operations, Travel and Operations Group.
- j. Certification Clause for reconciled SOAs: By affixing his/her required dated signature and printed name on the reconciled SOA, the cardholder and AO are certifying that the items listed on the SOA:
- (1) Are correct and proper for payment;
 - (2) That funds were available from the appropriate account prior to purchase;
 - (3) That the payment was legal, proper and correct including compliance with all agency and government-wide policies and procedures related to purchase card use;
 - (4) That all supporting documentation for each purchase will be retained for a period of five years; and,
 - (5) That the cardholder and AO understand that transactions on the reconciled SOA may be subject to periodic audit or inspection.
- Any exceptions to the Certification Clause must be noted on the SOA itself by the cardholder or AO, with the remarks being initialed and dated.
- k. Cardholders are required to maintain accurate and complete records to support all purchase card transactions. Supporting documentation may include invoices, receipts, vouchers, forms, a purchase card log, any written or emailed correspondence regarding the purchase decision, etc. in order to provide a complete audit trail of purchases upon review.

- l. All cardholders may be subject to periodic and/or indiscriminately selected reviews of their purchase card transactions and purchase practices by the APC, independent auditors working on behalf of the Office of Financial Operations or Managing Director, the FCC Office of Inspector General, and other federal entities charged with duties that include purchase card audits and investigations. Cardholders must fully comply with such reviews, audits and investigations by providing in a timely manner all supporting documentation and record(s) of purchases that are subject to review.
- m. Cardholders are directly responsible for furnishing copies of their reconciled SOAs and all other supporting documentation to auditors and reviewers of the purchase card program. Cardholders should not forward such document requests to a third-party in their organization, nor should they refer the reviewer/auditor to a centralized source. While copies of the cardholder's reconciled SOAs and supporting documentation are permitted to be centralized in any manner suitable to their organization, the cardholder is ultimately responsible for compliance with the reviewer's or auditor's request for documentation.

8. RESPONSIBILITIES:

- a. Managing Director: The Managing Director has agency-level responsibility for the administrative management of the FCC's Purchase Card Program.
- b. Chief Financial Officer (CFO): The CFO is responsible for ensuring timely review of all SOAs and receipts received from AOs, for distributing charges to correct financial and budgetary accounts, and for ensuring all reconciled purchase card transaction data are entered into the Commission's core financial accounting system.
- c. Bureau and Office Chiefs: Bureau and Office Chiefs who authorize personnel to receive and use a government purchase card bear the following responsibilities:
 - (1) Nominating cardholders and AOs for their respective organizations;
 - (2) Ensuring cardholders comply with all applicable regulations and procedures by promoting an environment that precludes cardholders from being pressured to make unauthorized purchases or to perform careless transactions, and permitting cardholders and AOs sufficient time to perform their purchase card responsibilities;
 - (3) Ensuring that budget allocations are sufficient to cover purchase card transactions, and instituting and maintaining appropriate procurement controls; assigning responsible, trained employees to procurement-related activities; and ensuring compliance with federal statutes and regulations, including the Anti-Deficiency Act (31 U.S.C. §§ 1341, 1342, and 1512);
 - (4) Monitoring cardholder and AO performance and periodically reviewing cardholder and AO assignments to verify continued participation of individuals in the program;
 - (5) Ensuring there is an appropriate cardholder/AO relationship to determine independence and separation of responsibilities, that the chain of command is appropriate for the transactions approval process, and that the cardholder and AO are cognizant of their fiduciary responsibilities and potential liability;

- (6) Ensuring that cardholders reconcile their the SOAs and forward them to their AO, and that AOs submit the reconciled SOAs to the Office of Financial Operations, Travel and Operations Group, in a timely manner proscribed by agency purchase card policy;
 - (7) Establishing a review process that ensures that procedures are being applied consistently, and following up and bringing to closure all reports of deficiencies in purchase card use within their organizations;
 - (8) Exacting appropriate disciplinary action in conjunction with Human Resources/Labor Relations and Performance Management in cases of purchase card fraud/misuse; and
 - (9) Providing changes in cardholder status to the APC, including terminations, changes of cardholders, etc., to ensure accurate and current records.
- d. Agency Program Coordinator (APC): The APC, as the agency's charge card manager, is responsible for oversight of the FCC's Purchase Card Program, including its day-to-day operations. The APC establishes and maintains operational procedures and guidelines. Serves as the liaison between the FCC and the contractor bank. Serves as the focal point for coordination of purchase card applications. Implements and monitors compliance with required training for cardholders, AOs and other entities as required. Issues and destroys cards; opens and closes accounts, and generates reports to detect fraud and abuse/misuse within the program.
- e. Approving Official (AO): The AO is responsible for oversight of the purchase card activity of cardholders under his or her purview. The AO is typically the cardholder's immediate supervisor, or a higher-level official in the cardholder's chain of command. A cardholder cannot be their own AO; nor can an AO be a subordinate of a cardholder. Contractors shall not be appointed as AOs.

The AO bears the following responsibilities:

- (1) AO nominees shall submit a certificate of completion of cardholder training (the same training required of purchase cardholder nominees) to the APC;
- (2) Authorizes each purchase card transaction before the purchase is made;
- (3) Validates receipt of items purchased, as applicable, prior to the cardholder's receipt and shall affix his/her signature on the receipt or invoice received with the shipment;
- (4) Reviews and reconciles cardholder(s)'s monthly SOAs within seven (7) workdays after the end of the billing cycle to verify that all transactions made with the purchase card were legal, proper, correct and necessary government purchases in accordance with the FAR and all other governing agency policy and procedure. Upon reconciling the SOA, the AO affixes his/her signature and printed name and date as certification that charges are for purchases which have been authorized and made in accordance with the FAR and other agency policy and procedure, and then forwards the reconciled SOA to the Office of Financial Operations, Travel and Operations Group;
- (5) Serve as liaison with the APC and the Office of Financial Operations, Travel and

Operations Group;

- (6) Assist the cardholder in resolving disputed payments;
 - (7) Direct the APC in writing (may be via email) to instruct the APC to cancel the card of a resigned or re-assigned user at any time; and
 - (8) Ensure that each cardholder has a copy of these and other required procedures and that the cardholder uses and demonstrates an understanding of the requirements for use of the government purchase card.
- f. Cardholder: The cardholder holds primary responsibility for their card's proper use. The cardholder is responsible for maintaining custody of the assigned purchase card and for making purchases in accordance with procedures contained in this directive. Each cardholder shall:
- (1) Cardholder nominees: Submit a completed bank card application form to Travel and Operations Group for submission to the contractor bank;
 - (2) Cardholder nominees: Submit a certificate of completion of cardholder training and completed *FCC Form A-498 Purchase Card Program Application for Cardholder and/or Approving Official* signed by their Bureau/Office ABC and their AO. The cardholder may not make any purchase card acquisitions until he/she has completed formal purchase card training under the auspices of the APC;
 - (3) Completes all required ongoing cardholder training, including refresher training. Cardholders must ensure all training certificates are available for review as requested by the APC, AO, or auditors;
 - (4) Maintains the physical security of the card. If the card is lost or stolen, the cardholder must immediately notify the purchase card contracting bank, the AO and the APC;
 - (5) Ensures availability of funds prior to initiating a purchase with the card. Failure to secure adequate funding may result in an Anti-Deficiency Act violation;
 - (6) Completes and attaches the *Section 508 Determination and Findings for Purchase Requests Form* if the item is one covered by the accessibility regulations affecting information technology (IT) products and services;
 - (7) Completes all other FCC purchase card-related form(s) for each transaction, as instructed by the cardholder's AO. Aside from the *Section 508 Determinations and Findings Form* and a reconciled SOA signed and dated by cardholder and AO in accordance to the Certifying Clause contained in the Policy section of this directive, the agency does not require any other forms to be completed to support the purchase card transaction. However, AOs, at their discretion, may determine the need for their cardholders to complete the form(s) listed below. Cardholders may still choose to voluntarily complete any of the various forms as a means of managing and organizing their purchase card activity. The forms below are available at <http://intranet.fcc.gov/omd/hrm/fccforms.html>.
 - *Form A-496 Record of Credit Card Orders Place by Telephone*;

- *Form A-521 Notice of Credit Card Purchase;*
- *Form A-526 Purchase Card Checklist;*
- *Form A-527 Record of Competition in Purchase Card Acquisitions for Items over \$3,000.*

- (8) Cardholder shall reconcile his/her monthly SOA received from the contractor bank within five (5) workdays after the end of the billing cycle. Upon reconciling the SOA, the cardholder must affix his/her dated signature and printed name on the reconciled SOA and forward it to his/her AO for review;
- (9) Retains copies of each reconciled SOA, as well as all supporting documentation for purchase transactions for a period of five (5) years after payment. FAR § 4.805(b)(3) states that records at or below the simplified acquisition threshold are to be retained for 3 years. (See Exhibit 1) However, the FCC augments the FAR by imposing a retention requirement of five years;
- (10) Notifies the APC prior to reassignment to another FCC organization or leaving the agency;
- (11) Transfers purchase card files in accordance with the AO's directions when the cardholder account is cancelled. All purchase card files must be available for review even after departure of the cardholder;
- (12) Ethical Understanding: The government purchase card bears the cardholder's name and shall only be used by the named cardholder for authorized U.S. government purchases or payments. Cardholders who make unauthorized purchases, allow others to use the card, or carelessly use their purchase card may be liable to the government for the total dollar amount of unauthorized purchases made in connection with the misuse or negligence. The cardholder may also be subject to disciplinary action under FCC directives or regulations, and other applicable federal law.

9. SPAN OF CONTROL FOR AGENCY PROGRAM COORDINATORS AND APPROVING OFFICIALS:

- a. As an internal management control, APCs and AOs must have spans of control that do not exceed levels that allow them to carry out their duties and responsibilities accurately and completely. Program officials must ensure the proper allocation of resources is committed to effectively manage the program.
- b. An APC will not manage more than three hundred (300) cardholders and AOs unless a written justification is approved by the Chief Financial Officer. The justification must request a not-to-exceed threshold of cardholder accounts to manage, and justify how the APC can effectively manage and control the requested threshold of accounts.
- c. An AO will not manage more than eight (8) cardholder accounts unless approved by the APC. The justification must request a not-to-exceed threshold of cardholder accounts to manage, and justify how the AO can effectively manage and control the requested threshold of accounts and properly perform all AO responsibilities.

10. UNAUTHORIZED USE OF THE PURCHASE CARD:

- a. Certain items may not be purchased with the government purchased card. Prohibited purchases include but are not limited to:
- (1) Split purchases. Refer to the definition of split purchases in the Definitions section of this directive. If a purchase requirement exceeds the cardholder's single purchase limit, the cardholder is not permitted to buy the items with his/her purchase card and must forward the requirement to EAC;
 - (2) Purchases of Information Technology. This includes the purchase of computer hardware, equipment, storage devices, software, software licenses, or any computer accessories under any circumstances including items such as laptop computers, notebooks, electronic tablets, electronic book readers, smartphones, smartphone/electronic tablet apps, thumb drives, modems and routers. Only the ITC is authorized to make these purchases on the Bureau/Office behalf. Regardless of their dollar value, all items of this nature must be purchased through the ITC. In addition, software licenses require a legal review by the Office of General Counsel (OGC), which is coordinated by EAC. For further guidance on computer-related purchases, email ITProjectRequests@fcc.gov;
 - (3) Recurring purchases. Recurring purchases should be placed under contract with EAC. Recurring purchases can be paid by purchase card only after a contract is in place; and the contract stipulates that the purchase card is an acceptable form of payment;
 - (4) Professional services. Services ranging from Equal Employee Opportunity (EEO) services to language interpretation to pest control services can be paid by purchase card only after a contract is in place and the contract stipulates that the purchase card is an acceptable form of payment.
 - (5) Purchases from foreign vendors, unless no other U.S. source is available. The cardholder must then provide supporting documentation to show that he/she conducted market research and could find no U.S. source;
 - (6) Alcoholic beverages; betting, casino gaming chips, or off-track betting;
 - (7) Cash advances, including money orders and travelers' checks;
 - (8) Construction services, including new construction, modifications and repairs;
 - (9) Dating or escort services, court costs, child support or alimony;
 - (10) Food or beverages for an agency event/function, until OGC has reviewed the circumstances for the purchase and has provided an opinion in advance that finds that the purchase will be in line with the narrow exceptions contained in GAO's Principles of Federal Appropriations Law;
 - (11) Purchase of meals, lodging, travel tickets, or bottled water (except if the water has been assessed non-potable or available drinking water poses health risks);

- (12) Hotel rooms for individual use. However, rental of conference/meeting rooms at hotels is authorized. Note, the government cannot purchase food for conference attendees unless the purchase is incidental to renting the room. In this situation, where a food purchase is required to obtain the conference room, the cardholder must document the food being purchased is the minimum amount required for the room rental;
 - (13) Gift certificates and gift cards. Gifts or mementos for individuals upon retirement or departure from the agency;
 - (14) Transactions with political organizations. Payment of individual memberships in private organizations (unless it is a professional organization that the Commission would normally pay for on behalf of the cardholder);
 - (15) Long-term lease of land or buildings: Use of the government purchase card to lease real property (i.e., land and/or buildings) for a term longer than one month is prohibited;
 - (16) Rental or lease of motor vehicles, land, or buildings (except for the rental or lease of a vehicle in order to transport government-owned, or seized, equipment of large or irregular size or the rental of secure storage for such items);
 - (17) Purchase of fuel, supplies, or repairs for agency fleet vehicles. The fleet vehicle's fleet charge card should be used for this purpose;
 - (18) Purchase of personal clothing or footwear, except in emergency situations when required for safety);
 - (19) Payment for telephone calls (except for the Enforcement Bureau in pre-authorized cases);
 - (20) Payment of salaries and wages;
 - (21) Tax payments. Payment of fines or penalties. Payment of parking fees (except when required to secure vehicles carrying government-owned, or seized, equipment, under (16) above);
 - (22) Travel related purchases (travel cash advances and payment of travel vouchers). This includes rental/lease of motor vehicles associated with official TDY travel supported by travel authorizations, purchase of meals, drinks, lodging, or other travel or subsistence costs associated with official government TDY travel that will be reimbursed on a travel voucher.
- b. Purchases from the following categories of merchants are prohibited, per this directive. The list of prohibited merchants includes but is not limited to:
- (1) Travel agencies; airlines or airports; hotels or motels (except for conference facilities; for other exceptions, consult with the APC);
 - (2) Courier services; telephone or other utility companies (except for EB Field Offices);
 - (3) Beer and wine stores, liquor stores; restaurants or bars; amusement parks/facilities or recreation services;

- (4) Pharmacies or drug stores; medical services/facilities (unless made on behalf of the Commission as determined by the agency Health and Safety Officer);
- (5) Schools or day-care facilities.

11. PENALTIES:

Cardholders and AOs must adhere to the policies contained in this directive, federal statutes and regulations, and all other government purchase card policies and procedures of the FCC. A violation of this directive or other purchase card policies and procedures will be referred to the cardholder's supervisor, Assistant Bureau Chief for Management (ABC) and the Chief, Labor Relations and Performance Management for appropriate administrative and/or disciplinary or adverse action.

If disciplinary or adverse actions are proposed, these actions will follow the normal progression through Human Resources as stated in the Basic Negotiated Agreement (for bargaining unit employees), Article 35 (Disciplinary Actions) and Article 36 (Adverse Actions) and the FCC Personnel Manual (for non-bargaining unit employees), Chapter 751 (Disciplinary Actions) and Chapter 752 (Adverse Actions).

12. DISPUTING A CHARGE:

- a. A dispute is a questionable transaction. The most prevalent dispute is an unauthorized order, but other examples include credit not received, alteration of amount charged, duplicate processing, and charges for orders that were cancelled.

Cardholders should first attempt to resolve the disputed transaction directly with the merchant. If unable to resolve the dispute with the merchant, the cardholder shall initiate a dispute the purchase card contractor bank (JP Morgan Chase Bank) within 60 calendar days from the date of the billing statement containing the transaction. Failure to protect the government's interest by timely initiating disputes can result in administrative or disciplinary action. Cardholders shall track disputes to completion.

Before disputing a charge:

- (1) Review the receipts, for example the transaction in question may have posted to the SOA with a different merchant name.
 - (2) If the cardholder's research confirms this is a dispute, the cardholder shall contact the merchant in an attempt to resolve the disputed charge. Cardholder shall document the actions taken to resolve the issue.
 - (3) If unable to resolve the dispute with the merchant, the cardholder shall immediately proceed with a dispute request with the contractor bank.
- b. Disputes regarding shipping charges and taxes can only be resolved with the merchant. If these charges are disputed or should not have occurred, the cardholder is responsible for obtaining a credit from the merchant. Shipping and tax charges are not disputable with the contractor bank.

13. CARD SECURITY:

It is the cardholder's responsibility to safeguard the purchase card and account number at all times. The purchase card should be kept in a locked file cabinet, safe, or other securely locked area. The Commission will not be liable for any purchase card transaction made by a person other than the designated user for that card. The cardholder shall immediately report lost or stolen purchase cards to the purchase card contractor bank, and notify both the AO and the APC.

14. SEPARATION OR TRANSFER OF CARDHOLDER OR APPROVING OFFICIAL:

- a. Cardholder: If the cardholder transfers within the agency or separates from the agency, the APC shall be notified immediately by the cardholder's AO, supervisor or Bureau/Office ABC. The cardholder shall surrender their purchase card to their AO or the APC, and transfer purchase card files in accordance with the AO's instructions. Cancellation of a cardholder's account also automatically results in the cancellation of the cardholder's delegation of procurement authority. No one other than the individual whose name is printed on the card is authorized to use the card.
- b. AO: Upon the separation or transfer of an AO, a new AO will be named by the appropriate Bureau/Office Chief to assume the review and certification duties of the previous AO. This change in official assignment shall be sent in writing to the APC.
- c. APC: Upon being notified about a cardholder's transfer or separation from the agency, the APC shall close the cardholder's account.

15. ETHICAL CONDUCT:

To ensure that every citizen can have complete confidence in the integrity of the Commission, each Commission employee shall adhere to the Commission's Code of Conduct (Code of Conduct) set forth in FCC Directive FCCINST 1102.5 "Policy for Detecting and Deterring Fraud and Promoting Ethical Conduct Within the Federal Communications Commission" with regard to activities relating to acquisitions purchased with the government purchase card. The Code of Conduct is designed to deter wrongdoing and promote, among other things, (a) compliance with applicable governmental laws, rules, and regulations; and (b) the prompt internal reporting of violations of the Code of Conduct to an appropriate person or persons identified herein. All employees shall report instances of suspected irregularities to the Commission's Office of Inspector General in accordance with Directive FCCINST 1102.5.

16. FOR ADDITIONAL INFORMATION:

For additional information concerning the FCC's Purchase Card Program, contact Rob Fream, Agency Program Coordinator, at (202) 418-0408, or rob.fream@fcc.gov.

17. EFFECTIVE DATE AND IMPLEMENTATION:

This directive is effective immediately and shall be implemented promptly upon distribution.

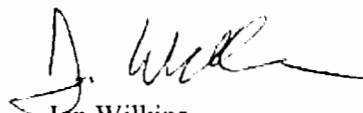

Jon Wilkins
Managing Director

Exhibit 1**FAR Subpart 4.8 Government Contract Files****48 CFR 4.805 Storage, handling, and disposal of contract files.**

b) If administrative records are mixed with program records and cannot be economically segregated, the entire file should be kept for the period of time approved for the program records. Similarly, if documents described in the following table are part of a subject or case file that documents activities that are not described in the table, they should be treated in the same manner as the files of which they are a part. The retention periods for acquisitions at or below the simplified acquisition threshold also apply to acquisitions conducted prior to July 3, 1995, that used small purchase procedures. The retention periods for acquisitions above the simplified acquisition threshold also apply to acquisitions conducted prior to July 3, 1995, that used other than small purchase procedures.

Document	Retention Period
(1) Records pertaining to Contract Dispute Act Actions.	6 years and 3 months after final action or decision for files created prior to Oct. 1, 1979, 1 year after final action or decision for files created on or after Oct. 1, 1979.
(2) Contracts (and related records or documents, including successful proposals) exceeding the simplified acquisition threshold for other than construction.	6 years and 3 months after final payment.
(3) Contracts (and related records or documents) at or below the simplified acquisition threshold for other than construction.	3 years after final payment.
(4) Construction contracts:	
(i) Above \$2,000.	6 years and 3 months after final payment.
(ii) \$2,000 or less.	3 years after final payment.
(iii) Related records or documents, including successful proposals, except for contractor's payrolls.	Same as contract file.
(iv) Contractor's payrolls submitted in accordance with Department of Labor regulations, with related certifications, anti-kickback affidavits, and other related papers.	3 years after contract completion unless contract performance is the subject of an enforcement action on that date.
(5) Solicited and unsolicited unsuccessful offers, quotations, bids, and proposals:	
(i) Relating to contracts above the simplified acquisition threshold.	If filed separately from contract file, until contract is completed. Otherwise, the same as related contract file.
(ii) Relating to contracts at or below the simplified acquisition threshold.	1 year after date of award or until final payment, whichever is later.
(6) Files for cancelled solicitations.	5 years after cancellation.
(7) Other copies of procurement file records used by component elements of a contracting office for administrative purposes.	Upon termination or completion.
(8) Documents pertaining generally to the	Until superseded or obsolete.

contractor.	
(9) Data submitted to the Federal Procurement Data System (FPDS). Electronic data file maintained by fiscal year, containing unclassified records of all procurements other than simplified acquisitions, and information required under 4.603.	5 years after submittal to FPDS.
(10) Investigations, cases pending or in litigation (including protests), or similar matters.	Until final clearance or settlement, or, if related to a document identified in (b)(1)-(9), for the retention period specified for the related document, whichever is later.

Federal Communications Commission Washington, D.C.	Title	
	Policy for Detecting and Deterring Fraud and Promoting Ethical Conduct within the FCC	
	Directive Number: FCCINST 1102.5	Effective Date: July 30, 2011

FCC Directive

1. PURPOSE: This directive sets forth the Federal Communications Commission's ("Commission" or "FCC") policies, procedures, and responsibilities relating to fraud and promoting ethical conduct within the Commission. The overall objective of the directive and the Commission's anti-fraud program is to ensure public confidence in the Commission by (1) preventing fraud; (2) detecting and removing existing fraud; and (3) promoting ethical conduct among Commission employees.

2. SCOPE: This directive applies to all Bureaus and Offices within the FCC.

3. FRAUD:

A. DEFINITION:

Fraud. Fraud refers to any intentional act designed to deprive the Commission unlawfully of something of value or to secure from the Commission a benefit, privilege, allowance, or consideration to which one is not entitled. Such practices include:

- (a) Fraudulent agency financial reporting, such as overstating assets or understating liabilities;
- (b) Misappropriation of assets, such as embezzlement, payroll fraud, and theft;
- (c) Incurring expenditures and liabilities for improper purposes, such as offering payment or accepting bribes or gratuities and arranging for secret profits, kickbacks, or commissions;
- (d) Fraudulently obtaining revenue and assets, such as committing a fraud against other employees or third parties;
- (e) Intentionally making false or misleading statements to auditors or investigators;
- (f) Submitting false claims against the Commission;

- (g) Evading or corrupting inspectors, auditors, or other officials; or
- (h) Deceiving either by suppressing the truth or misrepresenting material fact.

B. POLICY:

This directive establishes an internal control framework to detect and deter fraud within and against the Commission. The internal control framework described here consists of these six separate and distinct components: (1) control environment; (2) Commission Whistleblower Program; (3) Fraud Prevention Oversight Council; (4) investigation of alleged fraud; (5) fraud risk assessment; and (6) monitoring. In some instances, this directive merely reiterates Commission policy or restates applicable legal standards that are already in place, such as the Inspector General Act of 1978, as amended. By consolidating such practices, requirements and policies in one common document, this Directive will foster understanding of these principles and further promote an environment where fraud is deterred and ethical conduct is promoted.

The following points are FCC policy:

1. Control Environment. The purpose of anti-fraud internal controls is to ensure that an appropriate and operational program is in place to detect and deter fraud. The Commission's anti-fraud internal controls implement applicable statutes, regulations, and other guidance related to internal controls, including the Federal Managers Financial Integrity Act of 1982 (FMFIA), and the revised General Accounting Office (GAO) Standards for Internal Control in the Federal Government. The internal controls shall be designed to provide reasonable assurance that the following objectives are being achieved:
 - (a) Reliability of agency financial reporting: Ensuring that transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements in accordance with generally accepted accounting principles, and that assets are safeguarded against loss from unauthorized acquisition, use, or disposition;
 - (b) Compliance with applicable laws and regulations: Ensuring that financial transactions are executed in accordance with (a) laws governing the use of budget authority and other laws and regulations that could have a direct and material effect on the financial statements, and (b) any other laws, regulations, and government-wide policies identified by the Office of Management and Budget ("OMB") in its accounting and audit guidance;
 - (c) Effectiveness and efficiency of operations: Ensuring that agency resources are being used in a manner which seeks the best value consistent with the agency mission and objectives, and that agency assets are safeguarded from fraud; and

- (d) Proper asset use: Providing reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of the Commission's assets.
- 2. Commission Whistleblower Program. The Commission shall maintain a Whistleblower Program to provide employees and others a means of communicating concerns about potential violations of the Code of Conduct (see section 4.B. below), including unethical behavior and actual or suspected fraud, without fear of retribution. The Program shall include a hotline that shall be administered by the Office of Inspector General ("OIG") and shall be prominently displayed on OIG's web page. As of the effective date of this Directive, the reports of potential violations of the Code of Conduct should be made to (202) 418-0473, or toll-free to (888) 863-2244, or through e-mail at hotline@fcc.gov. The existence of the Hotline shall be made a part of the anti-fraud training programs and awareness efforts.
- 3. Establishment of a Fraud Prevention Oversight Council. The Commission shall maintain a Fraud Prevention Oversight Council ("Council"). The council shall oversee the establishment of internal controls for deterring and detecting fraud, including financial reporting and the process by which management satisfies itself that the controls are working effectively. The Council shall also be responsible for assessing the risk of fraud by management and ensuring controls are in place to prevent, deter, and detect fraud. The Fraud Prevention Oversight Council shall be comprised of the same individuals as the Commission's Senior Management Council, which has been established pursuant to OMB Circular No. A-123.
 - (a) Control Activities. The Commission's Fraud Prevention Oversight Council shall evaluate annually whether appropriate internal controls have been implemented in any areas identified as posing a higher risk of fraudulent activity. In this effort, the Fraud Prevention Oversight Council shall evaluate whether the controls implemented are adequate to address all susceptible activities; whether these controls are properly designed for the purposes of detecting, deterring, and mitigating the particular fraud risk to be minimized; and whether these controls are being applied properly to sufficiently address the Commission's risk of fraud.
 - (b) Information and Communications. The Commission's Fraud Prevention Oversight Council shall evaluate annually the effectiveness of the information gathering by and the communication about the fraud prevention and awareness program. This effort shall address:
 - (1) The frequency and sufficiency of training and oversight provided to employees, agents, contractors, and their employees regarding how to prevent, detect, and deter fraud;
 - (2) The adequacy of capabilities to collect and share information about fraud across the Commission;

- (3) The manner by which the Commission communicates the results of any investigation or disciplinary actions taken;
 - (4) Activities monitoring potential override and circumvention of control features, such as using information systems to avoid control activities; and
 - (5) The ability to detect and investigate information system misuse, such as maintaining system logs for an adequate period to perform investigations.
- 4. Investigation of Alleged or Suspected Fraud. All allegations of fraud involving programs, persons, and organizations affiliated with the Commission shall be thoroughly and timely investigated. All allegations of fraud or other criminal acts involving programs, persons, and organizations affiliated with the Commission, including those discovered during reviews or audits, shall be referred to OIG immediately. In addition, and independent of any investigation or other action taken by OIG, management (including the Fraud Prevention Oversight Council as necessary) shall immediately take all appropriate steps to investigate and stop any ongoing fraud. This directive is not intended to supplant existing Commission rules or procedures governing the actions or activities undertaken by third parties in the course of participating in Commission proceedings or processes (e.g., spectrum auctions).
- 5. Fraud Risk Assessment. The Fraud Prevention Oversight Council shall annually assess the risk of fraud in or against the Commission, including the potential for fraudulent financial reporting, misappropriation of assets, and unauthorized or improper expenditures. The Fraud Prevention Oversight Council shall also consider the risk of fraud by senior management and shall use a systematic assessment process to fulfill this obligation. In conducting this assessment, the Fraud Prevention Oversight Council shall:
 - (1) Consider potential fraud schemes and scenarios;
 - (2) Assess risk on a Commission-wide level;
 - (3) Evaluate the likelihood and significance of each risk to the Commission;
 - (4) Assess the exposure arising from each of the categories of fraud risk;
 - (5) Evaluate deficiencies in the anti-fraud controls designed to prevent specific frauds to determine if such frauds constitute a material weakness; and
 - (6) Consider the risk of override of controls by management.

In addition, the Managing Director or his or her designee shall test the effectiveness of the risk assessment process for every activity in which there is an identified risk of fraud.

- 6. Monitoring. The anti-fraud controls shall be subject to ongoing and periodic performance assessments. Changes within the Commission, the experience of individuals implementing the controls, and the results of ongoing monitoring shall all be considered in evaluating the effectiveness of the controls. An evaluation of

the Commission's monitoring systems shall include management's responsibility for enforcement and monitoring of the anti-fraud program and policies; prompt and sufficient response to significant deficiencies and material internal control weaknesses; periodic comparisons of amounts recorded by the accounting system against physical assets; and responsiveness to recommendations to strengthen antifraud controls. Such assessments and evaluations shall be performed by the Fraud Prevention Oversight Council.

4. ETHICAL CONDUCT:

A. POLICY:

To ensure that every citizen can have complete confidence in the integrity of the Commission, each Commission employee shall adhere to the Code of Conduct ("Code of Conduct"). The Code of Conduct is designed to deter wrongdoing and promote: (1) full, fair, accurate, timely, and understandable disclosure in reports and documents; (2) compliance with applicable governmental laws, rules, and regulations; and (3) the prompt internal reporting of violations of the Code of Conduct to an appropriate person or persons identified herein.

B. EMPLOYEE CODE OF CONDUCT:

The Code of Conduct summarizes the general principles of ethical conduct set forth in the Uniform Standards of Ethical conduct for Employees of the Executive Branch at 5 C.F.R. § 2635.101(b)(1)-(14) to which Commission employees are already subject in full. It does not replace other laws, regulations, directives, or Commission rules, *see, e.g.,* 47 C.F.R. Part 19, that establish ethical responsibilities for employees.

These principles are summarized here to emphasize their importance to the Commission's anti-fraud program. In this context, these principles shall govern employee conduct expressly to prevent fraud against the Commission, such as in avoiding instances of conflict of interest or unauthorized disclosure of official information relating to procurement and disposal of proceedings before the Commission. Specifically:

- (1) Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws, and ethical principles above private gain.
- (2) Employees shall not hold financial interests that conflict with the conscientious performance of duty.
- (3) Employees shall not engage in financial transactions using non-public Government information or allow the improper use of such information to further any private interest.
- (4) Employees shall not, except pursuant to such reasonable exceptions as are provided by regulation, solicit or accept any gift or other item of monetary value from any person or entity seeking official action from, doing business

with, or conducting activities regulated by the Commission, or whose interests may be substantially affected by the performance or nonperformance of employee duties.

- (5) Employees shall put forth honest effort in the performance of their duties.
- (6) Employees shall make no unauthorized commitments or promises of any kind purporting to bind the Government.
- (7) Employees shall not use public office for private gain.
- (8) Employees shall act impartially and not give preferential treatment to any private organization or individual.
- (9) Employees shall protect and conserve Commission property and shall not use it for other than authorized activities.
- (10) Employees shall not engage in outside employment or activities, including (absent recusal from relevant Commission matters) seeking or negotiating for employment, that conflict with official Commission duties and responsibilities. Professional employees (*e.g.*, attorneys, engineers, economists, and accountants) of the Commission shall obtain approval before engaging in the outside practice of the same profession as that of their official position, whether or not for compensation, in accordance with the standards and procedures set forth in 5 C.F.R. § 3901.102. In no event, however, shall an employee engage in approved outside employment during his or her tour of duty.
- (11) Employees shall disclose fraud to appropriate authorities.
- (12) Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those such as Federal, State, or local taxes imposed by law.
- (13) Employees shall adhere to all laws and regulations that provide equal opportunity for all Americans regardless of race, color, religion, sex, national origin, age, or handicap.
- (14) Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the Code of Conduct set forth in this directive. Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the Uniform Standards of Ethical conduct for Employees of the Executive Branch. Whether particular circumstances create an appearance that the law or these standards have been violated shall be determined from the perspective of a reasonable person with knowledge of the relevant facts.

C. Employee Training and Awareness of the Code of Conduct. To promote the use and effectiveness of the Code of Conduct, the Commission shall implement a continuing agency-wide training program, tailored to the specific functions and missions of the FCC, designed to inform all employees, agents, contractors, and their employees of their role in the Commission's efforts to combat fraud, and the

high ethical standards they are expected to follow in performing their duties. Specifically:

- (1) The Office of General Council shall communicate the Code of Conduct at least annually to all employees, agents, contractors, and their employees through the employee handbook, policy manual, intranet, e-mail, or similar means.
- (2) Completion of a fraud prevention and awareness training session is required when employees enter on duty and prior to contractors performing any work under their contract. Employees, agents, contractors, and their employees that collect, disburse, track, or account for moneys received by or paid to the Commission shall be required to attend recurrent fraud prevention and awareness training at least annually thereafter; all other employees are encouraged to complete such annual training, but in any event shall be required to attend fraud prevention and awareness training on a periodic basis. Training will address the significance of the FCC's Code of Conduct, the Commission's intolerance for fraud, and each person's duty to communicate or report actual or suspected fraud.

5. RESPONSIBILITIES:

A. The Office of Managing Director will:

- (1) Establish procedures to ensure that training and awareness materials are developed on preventing and detecting fraud;
- (2) Establish and participate in the Fraud Prevention Oversight Council; and
- (3) Ensure that employees are notified annually of their rights under the Whistleblower Protection Act of 1989 ("WPA"), and what constitutes a prohibited personnel practice under the Civil Service Reform Act of 1978.

B. The Chief Financial Officer will:

- (1) Develop training and awareness materials on preventing and detecting fraud, and, in conjunction with the Performance Evaluation and Records Management (PERM), ensure that employees receive adequate training on a regular basis;
- (2) Chair the Fraud Prevention Oversight Council, and organize meetings on at least a quarterly basis; and
- (3) Provide, to the Commission's Senior Management Council: (a) regularly-scheduled verbal reports on the on the activities of the Fraud Prevention Oversight Council performed in accordance with section B of this Directive, and (b) a comprehensive written assessment on the activities of the Fraud Prevention Oversight Council performed in accordance with section B of this Directive on at least an annual basis.

C. Consistent with the Inspector General Act of 1978, as amended, the Office of Inspector General will:

- (1) Assess all allegations of fraud and investigate those allegations to the extent appropriate, including those involving or impacting:
 - (a) The Commission and its programs and field activities;
 - (b) The Chairman and the Commissioners;
 - (c) All contract and procurement actions awarded by the agency;
 - (d) All kickbacks or bribery involving Commission employees, the Chairman, the Commissioners;
 - (e) Agency finances or accounting services; and
 - (f) Any other matters that the Inspector General considers appropriate for investigation.
- (2) In addition, the Office of Inspector General will:
 - (a) Review allegations of contract fraud in Commission programs and activities, corruption, antitrust, collusive bidding, conflicts of interest, and standards of conduct violations reported to the Commission and ensure that the allegations are promptly referred to the appropriate agency when there are reasonable grounds to believe that a violation of law may have occurred;
 - (b) Ensure that suspected criminal misconduct affecting or involving Commission operations or activities, including theft of Government property and computer fraud, is promptly and thoroughly investigated;
 - (c) Promptly review and, if warranted, investigate significant security and criminal incident reports involving suspected fraud, corruption, antitrust, conflicts of interest, and standards of conduct violations;
 - (d) Serve as the principal point of contact with the Department of Justice, the Defense Criminal Investigative Service, and other criminal investigative agencies for cases involving contract fraud, corruption, violations of antitrust, conflicts of interest, and laws pertaining to employee standards of conduct such as the Whistleblower Protection Act and the so-called No Fear Act; and
 - (e) Keep the Chairman advised of all significant contract fraud, antitrust, and standards of conduct cases that warrant his or her attention and apprise him or her of significant developments as appropriate.

D. Bureaus and Offices will:

- (1) Promptly notify the OIG of any allegation involving potential fraud or misconduct, investigate such allegations of fraud, and take prompt corrective action in coordination with the OIG and OGC, as appropriate.

- (2) Ensure that employees are effectively detecting, reporting, and following up on suspected fraud, employee misconduct, or anticompetitive contractor practices when identified.

E. Employees will:

- (1) Remain alert for deficiencies in internal control; instances of suspected fraud and illegal acts; and violations of provisions of contracts or grant agreements. Employees should report all instances of suspected fraud or illegal acts directly to the Office of Inspector General. Employees are encouraged to make such reports directly to their supervisor or manager. Employees may also report to other appropriate officials. Examples of such officials include, but are not limited to, officials in the FCC OIG and OGC. Reports to OIG can be made by contacting the Waste, Fraud and Abuse Hotline at (202)418-0473, or toll free at (888)863-2244. In addition, such reports may be e-mailed to the Office of Inspector General at hotline@fcc.gov.
- (2) Complete fraud prevention and awareness training regarding their responsibility to detect and promptly report fraud and suspected criminal misconduct, and cooperate in the investigation and prosecution of fraud involving Commission operations or activities. Such training shall occur on an annual or periodic basis, depending on each employee's individual duties, as described in section 4.C (2), above.
- (3) Be on alert for conduct that suggests the possibility of contractor fraud, corruption, antitrust violations, collusive bidding, conflicts of interest, or violations of the standards of conduct by Government employees. All employees shall report instances of suspected contract irregularities, anticompetitive practices by contractors, and fraud or illegal acts to the Commission's Office of Inspector General.
- (4) Employees shall report suspected violations of the standards of conduct to the Commission's Office of General Counsel and may also report such violations to the Office of Inspector General if they feel the situation merits review by that office.

7. EFFECTIVE DATE AND IMPLEMENTATION. This directive is effective immediately and shall be implemented promptly upon distribution.


Mindy J. Ginsburg
Deputy Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Records Management Program	
	Directive Number: FCCINST 1110.2	Effective Date: July 1, 2015

(1) PURPOSE. This directive sets forth the authorities, policies, and responsibilities for the Records Management Program at the Federal Communications Commission (FCC).

(2) CANCELLATION. This directive supersedes FCCINST 1110.1 dated March, 2008.

(3) SCOPE. This directive applies to headquarters and field units.

(4) AUTHORITIES.

- a. Title 44 U.S.C. Section 3101 *et seq.* requires the head of each Federal agency to establish and maintain an active, continuing program for the economical and efficient management of all records of the agency.
- b. The National Archives and Records Administration (NARA) has an extensive set of regulations, policies and guidance statements which supports the implementation of the statutory mandate that every Federal agency must:
 - (1) Make and preserve records that contain adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities (44 U.S.C. § 3101).
 - (2) Establish and maintain an active, continuing program for the economical and efficient management of the records of the agency (44 U.S.C. § 3102).
 - (3) Establish safeguards against the removal or loss of records including making requirements and penalties known to agency officials and employees (44 U.S.C. § 3105).

- (4) Notify the Archivist of any actual, impending, or threatened unlawful removal or destruction of records and assisting in their recovery (44 U.S.C. § 3106).
- c. Every Federal agency is legally required to manage its records as evidence of the agency's actions. Specific legal requirements for records management specified in OMB Circular No. A-130 (Revised) include:
 - (1) Incorporate records management and archival functions into the design, development, and implementation of information systems, including providing for public access to records where required or appropriate.
 - (2) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.
 - (3) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records.
 - (4) Provide training and guidance as appropriate to all agency officials, employees, and contractors on their Federal records management responsibilities.
- d. The Managing Government Records Directive (Office of Management and Budget Memorandum 12-18) creates a framework and goals for a Federal government effort to achieve the benefits outlined in the Presidential Memorandum titled Managing Government Records.

(5) DEFINITIONS.

- a. Records: All information, regardless of medium or format, made or received by the FCC under Federal law or in connection with the transaction of public business, either preserved or appropriate for preservation because of their administrative, legal, fiscal or informational value.
- b. Recordkeeping System: A manual or electronic system that captures, organizes, and categorizes records to facilitate their preservation, retrieval, use, and disposition.
- c. Permanent Records: Those records that NARA appraises as having sufficient value to warrant continued preservation by the Federal Government as part of the National Archives of the United States, because the records have continuing value as documentation of the organization and functions of the

FCC or because the records document the nation's history by containing significant information.

- d. Temporary Records: Those records that are designated for either immediate disposal or for disposal after a specified period of time or an event, in accordance with a NARA-approved agency records schedule or the General Records Schedule. Temporary records may document business processes or document legal rights of the government or the public, document government accountability, or contain information of administrative or fiscal value. Depending on the type of record, the retention period may range from immediate destruction to many years.
- e. Unscheduled Records: Those records whose final disposition has not been approved by NARA. Unscheduled records are potentially permanent and must be treated as if they are permanent.
- f. Non-Record Materials: Federally owned informational materials that do not meet the statutory definition of records (44 U.S.C. § 3301) or that have otherwise been excluded from coverage. Excluded materials include extra copies of documents kept only for reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit.
- g. Personal Papers: Documentary materials of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of agency business. Personal papers are excluded from the definition of Federal records and are not owned by the Government.
- h. Retention Period: The length of time that records must be kept.
- i. Appraisal: The process by which NARA determines the value and the final disposition of Federal records, designating them either temporary or permanent.
- j. Disposition: Those actions taken regarding records no longer needed for the conduct of the regular current business of the agency.

6. POLICY. The FCC will

- a. establish and maintain an active records management program for the economical and efficient management and release of its records.
- b. collaborate with NARA in applying standards, procedures, and techniques to improve the management of records, promote the maintenance of those records of continuing value, and facilitate the maintenance and disposal of temporary records.

- c. make reasonable efforts to maintain records in formats or media that are reproducible for purposes of the Freedom of Information Act.
- d. establish effective management controls over the creation, maintenance, and use of records in any medium, including paper and electronic media, throughout their life cycle.
- e. ensure that the records management program provides adequate and proper documentation of the FCC's activities and ensure records in any medium can be accessed as needed and authorized.
- f. ensure that records received or created by the FCC will be systematically identified, appraised, and their NARA-approved retention periods published in a records control schedule. Space devoted to records and information will be kept to a minimum by retiring or disposing of records according to the records control schedules, and through application of information technologies.
- g. ensure that vital records will be identified, protected, and secured in locations geographically separated from the original records in accordance with the policies in FCCINST 1111.1, FCC Vital Records Program.
- h. comply with all records management regulations and policies issued by NARA, including the provisions of all records control schedules approved and issued by NARA.
- i. ensure that the laws, regulations, and policies that apply to records and information maintained and used by the FCC also apply to FCC records and information maintained and used on FCC's behalf by FCC contractors. All records created by FCC contractors shall remain the property of the FCC and cannot be used except as explicitly authorized in writing by the FCC.

7. RESPONSIBILITIES.

- a. The Chairman of the FCC delegates to the Managing Director the responsibility to establish and maintain an active, continuing records management program for all FCC records.
- b. The Managing Director delegates to the Performance Evaluation and Records Management (PERM) the responsibility for the FCC's records management program. This includes responsibility for the preservation of records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the FCC which is designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the FCC's activities. Specific responsibilities include:

- (1) Developing procedures and processes to assure complete documentation and to facilitate retrieval, selection, and retention of records of continuing value, and disposition of non-record materials.
- (2) Assisting bureaus and offices in the scheduling of all records to facilitate prompt and systematic disposal of temporary records and to ensure retention of records of value.
- (3) Transferring records to other agencies, the National Archives, Federal Record Centers, and commercial storage facilities.
- (4) Developing and implementing training to familiarize FCC staff with their records management responsibilities.
- (5) Serving as the FCC's Agency Records Officer, representing the FCC in records management meetings and negotiations with NARA, General Services Administration, Office of Management and Budget, Government Accounting Office, and other agencies, as well as commercial firms as appropriate.
- (6) Conducting reviews and evaluations of the FCC's records management program by making: (1) on-site inspections; (2) reviews of all Bureau/Office (B/O) records control schedules; and (3) reviews of B/O submissions of record holdings.

c. The Office of General Counsel is responsible for:

- (1) Providing legal advice and counsel on matters concerning records preservation and disposition.
- (2) Interpreting statutes, executive orders, and presidential memoranda affecting federal records management.
- (3) Reviewing interagency agreements between FCC and NARA for temporary storage of records in Federal Record Centers and commercial storage facilities.

d. Bureau/Office (B/O) Chiefs are responsible for:

- (1) Maintaining the integrity of records in the custody of their respective B/Os, whether physically located in FCC headquarters or field office installations.
- (2) Executing the elements of the records management program by establishing internal procedures for adhering to this directive, to

NARA regulations, and to procedures established to administer the program and ensure staff observance of established guidelines.

- (3) Appointing a staff member from their B/O to act as a records liaison with the PERM staff.

8. GENERAL PROCEDURES

a. Training

- (1) All new FCC employees and contractors are required to complete the agency's online records management training within 30 days of commencing employment at the FCC as part of the New Employees Orientation Learning Plan.
- (2) Refresher records training will be offered at the discretion of the Associate Managing Director - PERM.
- (3) B/O Records Liaisons will be provided with additional records management training to perform their duties. This training will be provided by NARA or the FCC Agency Records Officer (ARO).

b. Scheduling Records

- (1) All groups of federal records created or maintained by the FCC will be scheduled with NARA as soon as practical. Federal records must be maintained and cannot be destroyed until a schedule for those records is approved by NARA.
- (2) General Record Schedules (GRS), developed by NARA, will be used by the FCC. Proposed records retention schedules that differ from a GRS require a justification from the B/O proposing the schedule as to why a different retention period is required for business purposes. Variations from the GRS must be approved by PERM and by NARA.
- (3) If a records group is not covered by a GRS, the B/O overseeing the records will work with the PERM staff to develop a schedule for records within that group. The ARO will submit the proposed schedule to NARA for review and approval. Records within that group may not be destroyed until the schedule is approved by NARA.

c. Maintaining Paper Records

- (1) Only paper records that are frequently accessed by FCC staff or the public should be maintained in office space or file rooms within headquarters or field locations. Due to the cost of commercial office

space, alternatives to onsite paper file storage will be considered by B/Os where it is cost effective and does not disrupt normal business procedures. Such alternatives include scanning paper files to associate them with electronic databases or to house them on a shared-access drive on the FCC network.

- (2) Paper records that are not frequently accessed will be stored at an off-site records storage location (Federal Records Center or commercial storage facility) until the records are destroyed after their retention period (for temporary records) or are accessioned to the National Archives (for permanent records).
- (3) Federal records may not be removed from FCC premises by departing employees without approval from the ARO. Approval must be sought in writing by the employee wishing to remove the records.

d. Maintaining Electronic Records

- (1) Federal records that are in electronic form will be preserved by
 - a) collecting those records in a folder on the FCC network's shared drive with limited access permissions.
 - b) periodically copying records contained in FCC databases and information systems to NARA-approved backup media that will allow those records to be restored if needed or, if permanent records, transferred to NARA. In addition, permanent records must be in a format that meets the requirements of NARA Bulletin 2014-04, Revised Format Guidance for the Transfer of Permanent Electronic Records.
- (2) Electronic records residing in databases and information systems will follow the same retention schedules as similar paper records, under NARA's concept of media-neutral scheduling. Electronic records should only be maintained beyond their scheduled retention period for mission-essential business purposes.

e. Disposition of Records

- (1) Permanent records will be accessioned to the National Archives as soon as practical upon completion of the NARA-approved retention period for those records. At the time of accessioning, control of and responsibility for the records passes to NARA. Permanent records may be pre-accessioned to the National Archives prior to the end of the retention period; however responsibility for the records remains with the FCC.

- (2) Temporary paper records should be destroyed as soon as possible after the conclusion of their retention period, unless the B/O possessing the records must retain them for mission-essential business purposes, or a litigation or Congressional hold or a Freedom of Information Act (FOIA) request requires that the records be retained. Records should be disposed using the locked bins whose contents are shredded, or another method approved by the Security Operations Center.
- (3) Temporary electronic records should be deleted as soon as possible after the conclusion of their retention period, unless the B/O possessing the records must retain them for mission-essential business purposes, or a litigation or Congressional hold or a FOIA request requires that the records be retained. Temporary electronic records stored on external media will be retained until the conclusion of their retention period, at which time the records will be erased or the storage medium destroyed in accordance with FCC Information Technology procedures.
- (4) Non-record materials, including personal papers, may be disposed of in regular trash or recycling containers when no longer needed.


for Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	FCC Vital Records Program	
	Directive Number FCCINST 1111.1	Effective Date February 20, 2013

1. **Purpose:** The purpose of this directive is to establish and assign responsibility for an effective Vital Records Program in the Federal Communications Commission (FCC or Commission) as it relates to emergency preparedness. The Vital Records Directive includes procedures for identifying and protecting records that specify how the Commission will operate in case of an emergency or disaster; records vital to the continued mission critical operations of the FCC during and after an emergency or disaster requiring activation of continuity plans, and records needed to protect the legal and financial rights of the FCC and of persons affected by its actions. The Directive also includes procedures for making these documents accessible for use in emergency situations.
2. **Background:** The Federal Vital Records Directive originated in the 1950's as part of the continuity of government program. Currently, Executive Order 12656 defines agency responsibilities during a national security emergency. The changing threat environment, especially the increased risk of terrorist attack, has heightened awareness of the importance of protecting the information that government agencies need to continue their essential functions in the event of an emergency. Federal Continuity Directive 1 (FCD-1), dated February 2008, provides additional guidance.
3. **Applicability and Scope:** This directive applies to all FCC Bureaus and Offices. Pursuant to 36 CFR Part 1223, 1236 and FCD-1, a Vital Records program is required to identify and protect those records that specify how the FCC will operate and continue its essential functions in case of an emergency or disaster, those records vital to the emergency operations of the FCC during and after an emergency or disaster, and those records needed to protect the legal and financial rights of the FCC and those affected by its actions. The FCC must implement a Vital Records program that includes procedures for accessing records required to support critical activities and essential functions the organization performs when operating under abnormal business conditions and/or in a location other than the normal place of business.
4. **Authorities:**
 - a. Title 44 U.S.C Section 3101 et seq. requires the head of each Federal agency to establish and maintain an active, continuing program for the economical and efficient management of all records of the agency.
 - b. Title 36 CFR, Part 1223 – Management of Vital Records, which prescribes policies and procedures for establishing a program for the identification and protection of Vital Records needed for continuity of agency operations before, during, and after emergencies and needed to protect the legal and financial rights of the Federal Government and persons affected by government activities.
 - c. E.O. 12656, Assignment of Emergency Preparedness Responsibilities, November 1988, which defines particular functions the FCC must perform under a national security emergency.

- d. FCC Continuity of Operations Plan (COOP), dated April 2010.
 - e. FCC INST 1110.1, Records Management Program Directive, dated March 2007.
 - f. Federal Continuity Directive 1, dated February 2008.
5. **Definitions:** Other definitions used throughout this Directive can be found in Title 36, Code of Federal Regulations (CFR) Part 1223, Management of Vital Records and FCD-1.
- a. **Vital Records:** Vital Records are information systems and applications, electronic and hardcopy documents, references, and records, to include classified or sensitive data, needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions; and essential records needed to protect the legal and financial rights of the Federal Government and those affected by Federal Government activities. Vital Records include Emergency Operating Records and Rights and Interests Records.
 - b. **Vital Records Manager:** The Associate Managing Director, Performance Evaluation and Records Management (AMD-PERM) has been designated as the manager of the FCC's Vital Records Program.
 - c. **Emergency Operating Records:** Those Vital Records essential to the continued functioning or reconstitution of the FCC during and after an emergency. Included are emergency plans and directives, orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical agency operations, as well as related policy or procedural records that assist agency staff in conducting operations under emergency conditions and for resuming normal operations after an emergency.
 - d. **Rights and Interests Records:** These include Vital Records critical to carrying out the FCC's essential legal and financial functions, and vital to the protection of the legal and financial rights of individuals, licensees, stakeholders, etc. who are directly affected by the agency's activities. These records include those with such value that their loss would significantly impair the execution of essential agency functions, to the detriment of the legal or financial rights and entitlements of the agency and the affected individual(s). Examples of these records are accounts receivable files; contracting and acquisition files; official personnel records; Social Security, payroll, retirement, and insurance records; and property management and inventory records.
 - e. **Disaster:** An unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on agency operations.
 - f. **Emergency:** A situation or occurrence that warrants immediate action to save lives and protect property, public health, and safety. An emergency could disrupt normal FCC operations. Examples of an emergency are:
 - (1) Natural Disasters
 - (2) Man-made and Technological Hazards
 - (3) Civil Disturbances
 - (4) Terrorism
 - (5) Material Shortages
 - (6) Infrastructure Failures

- g. **Off-Site Storage:** A facility other than the FCC's normal place of business where Vital Records are stored for protection. This is done to ensure that the Vital Records are not subject to damage or destruction from an emergency or disaster affecting the FCC's normal place of business.

6. **Objectives:**

- a. To identify and protect those Emergency Operating Records that Bureaus and Offices need to continue mission critical operations and essential functions in case of an emergency or disaster.
- b. To identify and protect Rights and Interest Records dealing with the legal and financial rights of the Government and/or persons directly affected by the agency's actions.
- c. To ensure that a current inventory of these records located at contingency sites is readily available.
- d. To preserve and make accessible both categories of records in emergency situations within prescribed time frames.

7. **Requirements:** The FCC must implement a Vital Records program that includes:

- a. Procedures for identifying, protecting, controlling access to, and ensuring availability of, records and information systems.
- b. Procedures for accessing records required to support critical activities that the organization performs when operating under abnormal business conditions and/or in a location other than the normal place of business.
- c. Plans for establishing and maintaining a Vital Records inventory that identifies:
 - (1) requirements for proper labeling and handling of Vital Records,
 - (2) security precautions,
 - (3) frequency of updates, and
 - (4) provisions for access from remote locations.
- d. Plan for safeguarding of proprietary information in coordination with the FCC Chief Security Officer.
- e. An inventory system that identifies hard copy and electronic records by:
 - (1) series or system title,
 - (2) description,
 - (3) type,
 - (4) name of office and individual responsible,
 - (5) physical location of records, and
 - (6) date of latest update.
- f. Provisions to ensure protection against records damage or loss.
- g. Provisions for storing and maintaining records that include the following:
 - (1) Duplicate copies of hardcopy Vital Records and associated inventory must be maintained at separate locations to ensure access within four hours in any situation.


- (2) Records must be maintained in a medium that is most viable for readability under emergency conditions, including the appropriate hardware and software necessary to access the records.
- (3) Electronic record storage must meet the following requirements:
 - (a) Records must be stored and physically accessible at an alternative offsite facility located outside of the National Capital Region in addition to its original location.
 - (b) Information Technology (IT) staff must ensure electronic records are available to users within 12 hours of an emergency which affects accessibility of original electronic records at the original locations. Electronic files located at an offsite storage location must be physically accessible and delivered within four hours to the FCC's Alternate Facility by the appropriate IT staff. The IT staff then has eight hours to make the records available to staff.
 - (c) Records must be properly labeled and sorted to easily identify data,
 - (d) Records must be accessible to users who may not be operating within an FCC facility but have access to broadband Internet and reasonable personal computer equipment similar to that provided by the FCC.
 - (e) Records must be protected from environmental hazards such as water, fire, electromagnetism, excessive heat, excessive cold, humidity, and any other environmental hazard that could threaten the integrity of the data.
- (4) Storage/backup protection methods must be selected based on:
 - (a) evaluation of the effectiveness of the protection,
 - (b) cost,
 - (c) degree of risk for potential loss,
 - (d) physical susceptibility to destruction, and
 - (e) need for special environmental conditions for transport (if required), storage, and update.
- (5) Ability to retrieve records quickly during an emergency or disaster.
 - (a) It is imperative that Vital Records storage, maintenance and recovery plans be reappraised and reviewed at least annually to ensure that changing conditions are addressed and that records continue to be immediately accessible. The results of such reviews and/or exercises must be documented.
 - (b) A plan must be developed and maintained to recover records that are damaged in an emergency or disaster, regardless of media. This plan must include the priorities for restoring or recovering multiple damaged systems and the options for recovery and replacement. This plan must also include a resource list of local disaster recovery firms that can assist in restoration, and employee contact lists and Vital Records inventories which must be maintained at multiple off-site locations to facilitate their use. See Appendix C.
 - (c) Procedures must be developed for ensuring that contracting officers transmit requirements of this directive to contractors to ensure that information management policies, manuals, and mission-specific information requirements relating to Vital Records are clear under the terms of their contracts or in the mission-specific scope of work provided within the budgeting process.
 - (d) As soon as possible after activation of continuity plans, but in all cases within 12 hours of such activation, continuity personnel at the alternate facility must have access to hard copies of Vital Records and/or the appropriate media for accessing electronic Vital Records, such as:
 - i. A local area network.
 - ii. Electronic versions of Vital Records.
 - iii. Supporting information systems and data.
 - iv. Internal and external e-mail and e-mail archives.
 - v. Issued "IronKey" USB-port flash memory devices.

8. **Responsibilities:**

- a. **Managing Director** - The Managing Director is responsible for the overall FCC Records Management Program, which includes all Vital Records as defined in this directive.
- b. **Performance Evaluation and Records Management** – The Associate Managing Director, Performance Evaluation and Records Management (AMD-PERM) is the FCC Vital Records Manager. In addition, under authority delegated by the Managing Director, AMD-PERM is responsible for providing assistance and advice on records disposition matters to officials throughout the Commission. PERM shall:
 - (1) Develop Vital Records policies for Emergency Operating records as well as Rights and Interest records in accordance with this Directive.
 - (2) Develop and maintain an inventory of the Commission's Vital Records (both electronic and hard copy records) and provides this list to the Public Safety & Homeland Security Bureau at least annually.
 - (3) Maintain liaison with the National Archives and Records Administration (NARA) and other Federal agencies on matters affecting Vital Records.
 - (4) Provide assistance in obtaining space and security provisions for safeguarding Vital Records.
 - (5) Assist in the transfer of Emergency Operating and Rights and Interests records to a Federal Records Center or other suitable location.
 - (6) Ensure that locations where Vital Records are stored provide adequate protection and accessibility in accordance with National Fire Prevention Association (NFPA) 232, Standard for the Protection of Records.
 - (7) Provide for the safeguarding of proprietary information in coordination with the FCC Chief Security Officer. Classified and unclassified records must be handled in accordance with FCC Information Security Directive 1131.1.
 - (8) Perform a risk assessment to identify risks if Vital Records are retained in current locations and media and of reconstituting them if they are destroyed.
- c. **Associate Managing Director, Administrative Operations (AMD-AO)** – The AMD-AO shall:
 - (1) Act as liaison for the security aspects of maintaining Vital Records at Headquarters, Alternate Facility, and at storage sites.
 - (2) Work with the FCC Chief Security Officer to ensure that classified Vital Records are identified and appropriate storage, protection, marking, and access measures are taken to protect them.
 - (3) Ensure that contracting officers transmit requirements of this Directive to contractors to ensure that information management policies, manuals, and mission-specific information requirements relating to Vital Records are clear under the terms of their contracts.
- d. **Associate Managing Director, Information Technology Center (AMD-ITC); also known as the FCC Chief Information Officer (CIO)** is responsible for:
 - (1) Ensuring that FCC Vital Records in electronic form are stored in multiple physical locations to ensure that they are not affected by emergencies or disasters occurring in the Washington, DC metropolitan area. AMD-ITC is responsible for storage of all electronic media deemed critical to the FCC mission.
 - (2) Ensuring that FCC staff can access Vital Records in electronic media within 12 hours of an emergency or disaster at the FCC alternate facility. Note that some Vital Records may have specific recovery requirements as identified in Bureau and Office Vital Records inventories.
 - (3) Ensuring appropriate protections for Vital Records and for copies of those records.

- (4) Ensuring that procedures to recover Vital Records are exercised on an annual basis and the results of such exercises are documented.
 - (5) Reviewing recovery procedures for electronic Vital Records annually to determine their effectiveness in safeguarding those records and also to determine if different methods, procedures, and media can and should be used. This type of review should be documented and may be done when exercising recovery procedures.
 - (6) Ensuring that all Vital Records in electronic media are up to date. Vital Records data should be up to date at all physical locations and accurate within 48 hours of any modification unless otherwise provided. Some Vital Records may have more strict requirements as defined in Bureau and Office Vital Records inventories.
 - (7) Ensuring the Vital Records on electronic media are protected from environmental hazards such as fire, water/humidity, and electromagnetism or other threats that could harm electronic media. This includes dispersal to other agency locations or off site storage facilities. When determining protection methods, it is important to take into account special media needs.
 - (8) Identifying and having readily available equipment necessary to access Alternate Facility Vital Records regardless of location.
 - (9) Identifying records recovery experts and vendors to assist with records recovery at the Alternate Facility in the event of damage. The CIO may consider contingency contracts with entities local to the Alternate Facility to provide services if and when needed.
 - (10) Taking steps to initiate basic records recovery until records recovery experts and vendors can provide professional assistance.
- e. Public Safety and Homeland Security Bureau (PSHSB) - PSHSB is responsible for planning and coordinating continuity requirements, emergency management and preparedness activities, disaster and devolution management, and related activities within the FCC including Continuity of Operations (COOP) planning. Specifically, PSHSB is responsible for the following:
- (1) Maintain a COOP Plan, updated annually, that specifies how the FCC will perform its essential functions in an emergency requiring the relocation of key personnel.
 - (2) Ensure, in coordination with the Office of Managing Director, that a current copy of the Commission's Vital Records inventory is available at the Alternate Facility.
 - (3) Maintain a list, updated quarterly, of authorized individuals (the FCC Emergency Relocation Group and the FCC Devolution Emergency Response Group) who need access to Vital Records at the alternate facility during an emergency or disaster. This list must be kept up to date to reflect staff changes and reassignment of program responsibilities.
 - (4) Periodically review the Vital Records Directive to address any new issues that arise, update information, and identify additional Vital Records resulting from new functions or organizational changes and provide this updated information to PERM and the CIO.
 - (5) Ensure Bureaus/Offices develop plans and procedures for collecting Vital Records.
- f. Bureau and Offices – The Chiefs of the FCC's Bureaus and Offices (B/Os) are responsible for the following:
- (1) Identify the most critical activities and operations (essential functions) that the B/O must perform if it must operate under COOP or during any emergency or disaster situation.
 - (2) Identify the Vital Records that support those critical activities and operations such as delegations of authority, orders of succession, directory of critical personnel, organization charts, mission statements, agency directives, and directories for all field offices. Examples of such records are shown in Appendix A. B/Os are responsible for the collection and storage of all non-electronic media required for them to complete their FCC mission.
 - (3) Develop a complete inventory of the B/O's Vital Records based on the B/O COOP Mission Essential Functions and conduct at least annual reviews of the inventory for completeness,

- updating as necessary. This inventory should identify any special requirements, record locations, record medium, and instructions for accessing those records.
- (4) Identify records that contain information needed to protect the legal and financial rights of the FCC and persons directly affected by the actions of the FCC. Examples of such records are shown in Appendix B.
 - (5) Provide PSHSB and PERM with a complete list of all B/O vital records annually.
 - (6) Identify records that are not in electronic form on the FCC network (or cannot be made in electronic form on the FCC network) and create a procedure for properly handling these files that meet the definition of FCC Vital Records. If necessary, work with the OMD to locate storage space at the alternate facility.
 - (7) Provide individuals with any passwords or codes needed to access Vital Records.
 - (8) Develop and maintain a Vital Records plan packet. These packets shall be reviewed and updated annually. A copy shall be maintained at the agency's alternate facilities and other locations where it is easily accessible to appropriate personnel when needed. Each Bureau/Office must develop a Vital Records plan packet that includes:
 - (a) A hard copy or electronic list of key agency personnel and continuity personnel with up-to-date telephone numbers.
 - (b) A Vital Records inventory with the precise locations of Vital Records.
 - (c) Necessary keys or access codes.
 - (d) Alternate facility location(s).
 - (e) Access requirements and lists of sources of equipment necessary to access the records.
 - (f) A copy of the FCC and Bureau/Office COOP Plans.
9. **Disposition of Records:** Original Vital Records must be maintained by Bureaus and Offices for the periods of time specified in the FCC records disposition schedules and in accordance with the NARA requirements. Duplicate copies of Vital Records stored in alternate locations should be disposed when obsolete or superseded and replaced with an updated revision.
10. **Vital Records Training:** The Vital Records program must include a training program for the COOP Emergency Relocation Group (ERG); Devolution Emergency Relocation Group (DERG); and Bureau/Office Assistant Chiefs for Management. Training should focus on identifying, inventorying, protecting, storing, accessing, and updating the Vital Records.
11. **Vital Records Review:** The Vital Records program must be reviewed annually by the Public Safety and Homeland Security Bureau and the Office of Managing Director to address any new issues, identify problem areas, update information, and incorporate any additional Vital Records generated by new agency programs or functions or by organizational changes to existing programs or functions.
12. **Vital Records Testing:** The FCC must conduct tests of its capabilities for protecting classified and unclassified Vital Records and for providing ready access to them from the alternate facility at least annually. It is appropriate to conduct a review and capability testing of the Vital Records program in conjunction with continuity exercises.



David Robbins
Managing Director

Appendix A - Emergency Operating Records

The following examples of emergency operating records are found within most FCC bureaus and offices. In addition, FCC bureaus and offices may have other records that are considered emergency operating records. Any records that are considered to be emergency operating records should be forwarded to PERM for inclusion into the FCC Inventory of Vital Records.

- Bureau and Office Vital Records inventories;
- Emergency plans and directive(s), such as;
 - FCC COOP Plan;
 - FCC Pandemic Plan;
 - FCC Devolution Plan;
 - FCC Reconstitution Plan;
 - ITC Disaster Recovery Plan;
 - Occupant Emergency Plan;
 - Building systems operations manuals (HQ and Gettysburg)
- Emergency Relocation Group (ERG) staffing assignments;
- Contact information for all FCC staff, including home addresses and alternate telephone numbers. (All B/O's)
- FCC Operations Center checklists or standard operating procedures. (PSHSB)
- Orders of Succession
- Delegations of Authority
- Equipment inventories for all agency facilities. (AMD-AO)
- Program records (whatever the medium) needed to carry out continuing critical functions. (All B/O's).
- System documentation for any electronic information systems designated as emergency-operating records. (AMD-ITC)

Appendix B - Rights and Interests Records

The following are examples of legal and financial rights records. Any records that are considered to be legal and financial rights records should be forwarded to PERM for inclusion into the FCC Inventory of Vital Records.

- Accounts-receivable records. (AMD-FO)
- Accounts-payable records. (AMD-FO)
- Purchase Card Program Records – Cardholders and Card Approving Officials. (AMD-FO)
- Blanket Purchase Agreements. (AMD-AO)
- Financial Records of Operations. (AMD-FO)
- Personnel Records. (AMD-HRM)
- Memoranda of Understanding with other agencies. (AMD-AO)
- Memoranda of Agreement with other agencies. (AMD-AO)
- Payroll Records. (AMD-HRM)
- Insurance Records/Health/Life/TSP.(AMD-HRM)
- Retirement Records (AMD-HRM)
- Debts owed to the Government. (AMD-FO)
- Legal proceedings and decisions (OGC)
- Contract files (AMD-AO)

Appendix C – Data Recovery Services

If vital records are damaged in an emergency or disaster, the FCC may use one of the following vendors to assist in the recovery of records. The first priority will be to recover those records identified as “high” priority in the FCC COOP Plan.

Washington, DC Area

- **SalvageData Recovery Services**
1325 G Street NW, Ste 500
Washington, DC 20005
(202) 629-9884
www.salvagedata.com
- **Secure Hard Drive Raid Data Recovery Services**
1875 I St NW, 5th Floor
Washington, DC 20006
(202) 407-9400
www.securedatarecovery.com
- **TTR Data Recovery**
700 12th Street Northwest
Suite 700
Washington, DC 20005
(202) 652-4959
www.ttrdatarecovery.com

Pennsylvania Recovery Services:

- **Data Recovery PA**
2502 Horseshoe Road
Lancaster, PA 17601
717-656-2286
www.datarecoverypa.com/

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Paperwork Reduction Act Program	
	Directive Number: FCCINST 1112.1	Effective Date: July 2015

1. **PURPOSE:** This directive establishes the objectives and responsibilities of the Federal Communications Commission’s (FCC or Commission) program implementing the provisions of the Paperwork Reduction Act (PRA) of 1995, as amended, as well as any other related applicable Federal legislation and regulations concerning collections of information.
2. **SCOPE:** This directive applies to all bureaus and offices within the Commission with programs to maintain, retain, report or publicly disclose information collected from the public, regardless of the method used to collect such data.
3. **AUTHORITIES:**
 - a. The Paperwork Reduction Act of 1995, as amended (44 U.S.C. §§3501 *et seq*) and the Office of Management and Budget’s implementing regulations (5 C.F.R. §1320 *et seq*).
 - b. Clinger-Cohen Act of 1996, “Information Technology Management Reform Act,” (40 U.S.C. §11101 *et seq*).
 - c. The Small Business Paperwork Relief Act of 2002 (44 U.S.C. §§3504, 3506).
 - d. The Government Paperwork Elimination Act, Pub. L. 105–277.
 - e. Executive Order 12291, “Federal Regulation.”

4. **BACKGROUND:**

The Paperwork Reduction Act of 1995 establishes a process for the review and approval of information collections to:

- minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, federal contractors, state, local and tribal

governments, and other persons resulting from the collection of information by or for the federal government;

- ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the federal government;
- improve the quality and use of federal information to strengthen decision making, accountability, and openness in government and society;
- minimize the cost to the federal government of the creation, collection, maintenance, use, dissemination, and disposition of information; and
- ensure the integrity, quality, and utility of the federal statistical system.

In addition to the purposes above, the PRA identifies several other purposes relating to the management of federal information resources. These include coordinating information resources management policies and practices to improve the productivity, efficiency, and effectiveness of Government programs, improve service delivery to the public, and provide for the dissemination of public information on a timely basis.

An information collection must be cleared by the Office of Management and Budget (OMB) if an agency collects information from ten or more people by means of identical questions or identical reporting, regardless of whether the collection is mandatory, voluntary, or required to obtain or retain a benefit. Information collections that require clearance also include requirements to retain records as well as requirements to disclose information to an agency, third parties or the public.

The FCC's PRA program is intended to monitor, implement, review and report on PRA activities for the agency and to reduce the burden of collecting information from the public. The PRA program consists of:

- preparing and publishing an initial Federal Register notice ("60-day notice") notifying the public of the proposed information collection and soliciting comment;
- developing and submitting Form OMB 83-I, Paperwork Reduction Act Submission to request OMB approval of the collection;
- developing and submitting a supporting statement for the collection, responding to 18 questions prescribed by OMB;
- preparing and publishing a subsequent Federal Register notice ("30-day notice") notifying the public that the clearance request and supporting statement have been submitted to OMB and that there is an additional 30-day public comment period.

5. POLICY:

The following is Commission policy:

- a. The FCC will establish and maintain a program for the collection of information, administered by the Office of Managing Director's Performance Evaluation and Records Management (PERM).
- b. Collection of information will not become effective until the OMB has reviewed the proposed collection and assigned a control number to the collection. Under no circumstances may information be collected from the public without prior approval by OMB. Continued use of any collection of information after the expiration of an OMB-approved collection is not authorized or enforceable.
- c. To ensure compliance with all applicable Federal legislation, executive orders and OMB guidance, all Bureaus and Offices shall minimize the information collection burden imposed on the public in terms of the time, effort and/or financial resources expended to provide information to the Commission, while ensuring that all data necessary to accomplish the Commission's mission are requested and received in a manner most useful to the stated purpose.
- d. Only information essential to the implementation, conduct, or management of FCC programs or in pursuit of the FCC's mission will be collected. All collections will be periodically reviewed to determine if the information received is still needed. At a minimum this review will take place prior to extension of an information collection.
- e. Forms used in the collection of information will be electronically designed, whenever possible, for ease of interpretation, completion, transmittal, processing, and retrieval by persons with disabilities.

6. RESPONSIBILITIES:

- a. The Managing Director is the Senior Agency Official designated to carry out the responsibilities of the Commission under the Paperwork Reduction Act and the implementing regulations. As such, the Managing Director ensures that procedures are established to carry out the Commission's information management activities in an efficient, effective and economical manner, and comply with the information policies, principles, standards, and guidelines prescribed by the OMB and this Directive. The Managing Director shall also establish and oversee a program office that will review, evaluate, and process information collection requests proposed by individual offices and bureaus.

- b. The Associate Managing Director for Performance Evaluation and Records Management (PERM) is responsible for conducting the activities of the program in a prompt, efficient, and effective manner, including:
1. Acting as liaison with OMB for the submission of requests for review;
 2. Preparing agency directive(s) and other written instructions on all phases of the program;
 3. Making a determination, in response to inquiries from the bureaus and offices, whether a proposal falls within the purview of the PRA and therefore must be submitted to OMB for review. If an opinion is required regarding a final determination, the Associate Managing Director for PERM shall prepare a request to the General Counsel for a written legal interpretation and opinion, and shall notify the requesting Bureau or Office in writing of the determination;
 4. Providing guidance to the bureaus and offices in the preparation of the requests for OMB review;
 5. Reviewing all proposals to ensure that all necessary requirements and criteria have been met prior to submission of requests to OMB for review;
 6. Providing monthly notification to bureaus and offices of information collections due to expire during the next 120, 90, 60 and 30 days;
 7. Notifying the appropriate Bureau or Office Chief by letter, signed by the Managing Director, if the Bureau/Office has not taken action (*i.e.*, extension or revision) on an information collection that is 30 days from expiration;
 8. Overseeing Bureau/Office preparation of a notice for publication in the Federal Register to inform the public when an information collection has been submitted to OMB for approval;
 9. Overseeing Bureau/Office preparation of a notice for publication in the Federal Register to inform the public of OMB approval action on FCC forms, the expiration date, and the status of existing editions of revised forms;
 10. Periodically updating and amending 47 C.F.R. § 0.408, and OMB Control Numbers assigned pursuant to the Paperwork Reduction Act, which lists each section of the Commission rules containing an approved information collection requirement; and
 11. Coordinating all activities of the Paperwork Reduction Act program within the Commission.
- c. The Bureau/Office Chiefs are responsible for:
1. Implementing their respective information collection programs to ensure that the information collection requests accomplish the mission of their respective Bureau/Office;
 2. Ensuring compliance and implementation of responsibilities associated with the Paperwork Reduction Act of 1995, as amended;
 3. Providing guidance, support, and assistance to PERM regarding PRA requests and compliance, including:
 - a) Identifying any proposal (e.g., Notice of Proposed Rulemaking (NPRM), form, rule section, report, etc.) which contains a collection of information, as defined in 5 CFR 1320.7(c) and (d), and would impose a reporting, recordkeeping or

record retention requirement on the U.S. public.

- b) Requesting a determination from PERM, when necessary, as to whether such a proposal requires OMB review and approval in compliance with the PRA.
- c) Ensuring that the proposed information collection does not unnecessarily duplicate existing requirements.
- d) Estimating the public burden, as defined in 5 C.F.R. § 1320.7(b), to be imposed by any such proposal.
- e) Minimizing the public burden by ensuring the practical utility, as required by 5 C.F.R. § 1320.4(b)(3) and defined in 5 C.F.R. § 1320.7(q), to the Commission of all data collected, and providing justification for the data collection.
- f) Ensuring that each Agenda Item contains a PRA statement as required by the Commission Agenda Handbook.
- g) Determining whether the proposal is expected to have a significant effect on domestic small business, and evaluating alternatives to mitigate this impact, as required by 5 C.F.R. § 1320.6(h).
- h) Preparing necessary submissions Information Collection Budget as directed by OMB in 5 C.F.R. § 1320.10.
- i) Preparing the Request for OMB Review and supporting documentation, including any required justifications, on all proposed information collections for which the bureau or office is responsible.
- j) Ensuring that every currently approved information collection (*i.e.*, extension or revision) is submitted to PERM for processing to OMB at least 150 days prior to its expiration.
- k) Submitting the SF-83 package and letter to OMB when an information collection is requested for expedited or emergency review, along with a memorandum from the Bureau Chief to the Managing Director justifying the need for expedited or emergency review.
- l) Coordinating expedited Federal Register publication requests with the Office of the Secretary, including providing a cost estimate of the expedited publication and indicating whether the entire item or a portion thereof is to be reproduced.

d. The General Counsel shall:

- 1. Provide legal advice, interpretations and opinions on the PRA and the OMB regulations and compliance with the PRA and regulations; and
- 2. When requested by the Managing Director or his designee, provide a written opinion whether a proposed information collection is subject to the legal and statutory requirements of the Act, and/or whether the proposal is in compliance with the Act and OMB regulations.

For 
Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Compliance with Privacy Laws and Guidance	
	Directive Number: FCC INST 1113.2	Effective Date: April 2016

TO: All Employees

SUBJECT: Compliance with Privacy Laws and Guidance

Purpose. This Directive establishes the policy and assigns responsibilities for the Federal Communications Commission (FCC) regarding carrying out the requirements of the Privacy Act of 1974, as amended (Privacy Act), and of generally following good privacy practices in the management of the FCC. This Directive also authorizes issuance of a Privacy Act Manual containing detailed FCC policies, procedures and information requirements for implementing the Privacy Act. The Privacy Act Manual will be updated periodically, as necessary, to reflect changes in law, regulation, or Presidential guidance or Executive Order.

Scope. This Directive applies to all employees and is also applicable to contractors as a term of their contract with the FCC.

Authority. Privacy Act of 1974, 5 U.S.C. 552a; Federal Information Security Management Act of 2002, 44 USC 3541, *et seq.*; Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. 101, *et seq.*; Office of Management and Budget (OMB) memoranda (as listed and updated at http://www.whitehouse.gov/omb/inforeg_infopoltech#pg); and National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (as listed and updated at <http://csrc.nist.gov/publications/>).

Policy. An individual's privacy is a right that must be respected and protected. It is the policy of the FCC that all employees and contractors shall be made aware of, and comply with, the Privacy Act, and other applicable laws and guidelines addressing privacy, and that information about individuals shall be collected, maintained, used, disseminated, protected, and destroyed (when no longer needed or out-of-date) in accordance with the Privacy Act and FCC regulation and policy.

The FCC's Privacy Act Manual, incorporated by reference into the Directive, comprises the following modules:

CHAPTER 1	FCC PRIVACY POLICIES AND GENERAL PROVISIONS
CHAPTER 2	COLLECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)
CHAPTER 3	DISCLOSING PII IN RECORDS
CHAPTER 4	ACCESS, AMENDMENT, AND APPEALS BY INDIVIDUALS
CHAPTER 5	PRIVACY ACT EXEMPTIONS
CHAPTER 6	NEW, REVISED, OR CANCELLED SYSTEMS OF RECORDS
CHAPTER 7	EMPLOYEE PERFORMANCE RECORDS MAINTAINED BY SUPERVISORS
CHAPTER 8	INFORMATION SYSTEMS AND TECHNOLOGY GUIDELINES
CHAPTER 9	PRIVACY IMPACT ASSESSMENTS
CHAPTER 10	COMPUTER MATCHING PROGRAM GUIDELINES
CHAPTER 11	DATA INTEGRITY BOARD
CHAPTER 12	FEDERAL AGENCY WEBSITE PRIVACY POLICIES
CHAPTER 13	THIRD PARTY WEBSITES AND APPLICATIONS
CHAPTER 14	PRIVACY TRAINING
CHAPTER 15	FEDERAL INFORMATION SECURITY AND MANAGEMENT ACT (FISMA) PRIVACY REQUIREMENTS
APPENDIX 1	GUIDELINES FOR PROTECTING SOCIAL SECURITY NUMBERS AND PII
APPENDIX 2	OFFICE OF FEDERAL REGISTER SYSTEM OF RECORDS NOTICE (SORN) TEMPLATE
APPENDIX 3	OFFICE OF FEDERAL REGISTER MATCHING ACTIVITIES NOTICE TEMPLATE
APPENDIX 4	MATCHING ACTIVITIES CHECKLIST
APPENDIX 5	FCC WEBSITE PRIVACY POSTING REQUIREMENTS
APPENDIX 6	ADAPTED PRIVACY IMPACT ASSESSMENT (PIA) TEMPLATE
APPENDIX 7	OMB GUIDANCE ON ADAPTED PIA TEMPLATE
APPENDIX 8	SAOP ANNUAL FISMA PRIVACY REPORT
APPENDIX 9	FISMA PRIVACY ACTIVITIES REPORTING QUESTIONNAIRE

Responsibilities.

A. The Managing Director or his/her delegate shall:

- Oversee management of the FCC privacy program
- Designate a senior official (at the Assistant Secretary or equivalent level) as the Senior Agency Official for Privacy (SAOP) with agency-wide responsibility for information privacy issues, to ensure ongoing compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

B. The Senior Agency Official for Privacy (SAOP) shall:

- ensure implementation of information privacy protection, including full compliance with federal laws, regulations, and policies relating to information privacy;
- chair the Data Integrity Board (DIB) that oversees information sharing, computer matching, and related issues;
- review and approve all System of Record Notices (SORNs), Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs);
- oversee the annual Federal Information Security Management Act (FISMA) review with all Bureaus/Offices and submission of the Privacy section to OMB; and
- ensure employees and contractors receive appropriate training and education and information regarding privacy laws, regulations, policies and procedures governing the agency's handling of personally identifiable information (PII).

C. The Chief Information Officer or his/her delegate shall:

- Preserve and protect PII contained in FCC systems of records;
- Audit compliance with the requirements of this Directive and any related internal policies and procedures;
- Establish an internal FCC Data Integrity Board that shall oversee and approve use of computer matching programs;
- Establish training programs for FCC personnel and contractors to ensure ongoing compliance with privacy laws, regulations, policies, and procedures for handling PII;
- Designate an employee in FCC Information Technology (FCC IT) as manager of the FCC's privacy programs (the "Privacy Manager"); and
- Assist the Bureaus and Offices in the implementation of uniform and consistent policies and standards governing the acquisition, maintenance and use of computers or other electronic or telecommunications equipment in the collection, compilation, maintenance, use, or dissemination of Privacy Act records.

D. The Privacy Manager (PM) or the PM's designee shall Coordinate and manage the FCC's privacy program and, with input from the SAOP, ensuring:

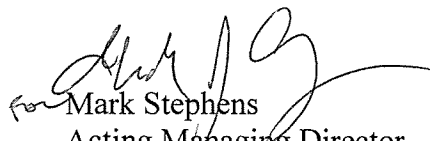
- FCC implementation of information privacy protections to ensure ongoing compliance with federal laws, regulations, and policies relating to information privacy;
- Management, coordination, and facilitation of FCC implementation of all privacy compliance efforts including annual FISMA submissions;
- FCC personnel and contractors receive appropriate training and education programs regarding privacy laws, regulations, policies, and procedures for handling PII;
- Implementation of all FCC Data Integrity Board activities;
- Revitalization of the strategic direction for the FCC privacy program;
- Review of proposed new, altered and amended systems of records;
- Development of Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) for new or modified systems; and
- Submitting required system of records notices (SORN) for publication in the Federal Register and, when required, provide advance notification to Office of Management and Budget and Congress.

E. Office of the General Counsel shall

- Provide advice and assistance on all legal matters related to the administration of the FCC privacy program.

F. Bureau and Office Chiefs (or their designees) shall:

- With guidance from the CIO and PM, ensure that employees and contractors are, at the required intervals, trained in, understand and follow the requirements of the Privacy Act in the performance of their official duties.
- With guidance from the CIO and PM, ensure that personnel who require access to PII are properly trained at the required intervals in the handling of such information.
- Provide the CIO and PM information on an ongoing basis regarding changes in collections of PII.


Mark Stephens
Acting Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Directives System	
	Directive Number: FCCINST 1114.1	Effective Date: August 9, 2013

1. **PURPOSE:** This directive sets forth the Federal Communication Commission's (Commission or FCC) policies, procedures, and responsibilities relating to drafting, modifying, amending, and implementing agency-wide policies, procedures, requirements, and other information through the use of directives. Directives are the primary means within the FCC to issue, establish, and describe agency policies, organization, responsibilities, methods, and procedures for internal activities. This directive does not affect the authority of any official to make substantive policy or issue regulations. It affects only the methods, formats, and procedures for ensuring uniformity, orderliness, and completeness in the promulgation and distribution of policy, including regulations.
2. **SCOPE:** This directive applies to headquarters and field units.
3. **AUTHORITY:** The Managing Director is authorized to administer directives under 47 C.F.R. §0.11(a)(2) of the Commission's rules.
4. **POLICY:**
 - A. The FCC Directives System utilizes two types of formats:
 - (1) **Directives.** These documents prescribe mandatory agency-wide policies. They may be permanent or temporary. If the policies are temporary, such as for one-time reports or data collections, specify the expiration or rescission date. In contrast to handbooks, directives should convey policies and should only discuss procedures to the extent necessary to explain the policies.
 - (2) **Handbooks.** These documents prescribe mandatory agency-wide procedures or operational requirements implementing policies contained in directives. Handbooks may be designed to add technical or procedural detail to requirements established in a related directive. Like directives, they may be permanent or temporary. If the procedures are temporary, such as for one-time activities, specify the expiration or rescission date.

- B. Identification and numbering of directives and handbooks will use a classification system based on subject rather than organization. The classification system and associated list of subjects will be maintained by the Associate Managing Director - Performance Evaluation and Records Management (PERM), and will be found on PERM's intranet page (intranet.fcc.gov/omd/perm).
- C. Documents published as part of the FCC Directives System should not repeat material published in Government-wide documents, such as by the Office of Personnel Management or Office of Management and Budget. FCC directives and handbooks should refer to those documents.
- D. FCC directives must follow established formats and procedures found in Appendix A.
- E. Directives and handbooks will be reviewed annually by the organizations that produced them in conjunction with the FCC internal controls program. If it is determined that a directive or handbook needs to be revised due to changes in policies or procedures, the revision will be scheduled for the following fiscal year. Pursuant to the FCC's implementation of Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, the head of each organization with responsibility for producing directives will certify in their annual internal controls assertion letter that all of their directives have been reviewed and identify those for which revision is required.
- F. Distribution of directives and handbooks is accomplished by electronic means only. The directives are posted to the FCC intranet and internet except for directives requiring special handling because of their sensitive content.

5. RESPONSIBILITIES:

- A. The Managing Director. The Managing Director oversees the directives management program and ensures its proper implementation. As such, the Managing Director will:
 - (1) Establish regulations and guidelines regarding the management of an effective FCC Directives System and ensure their implementation.
 - (2) Evaluate all phases of directives activities within the agency and implement changes as appropriate.
- B. Performance Evaluation & Records Management (PERM). The Associate Managing Director overseeing PERM shall:
 - (1) Develop and recommend guidelines to implement the FCC directives management program.

- (2) Oversee the subject classification table and assign numbers for all directives.
- (3) Recommend improvements to proposed and existing directives.
- (4) Ensure all bureaus and offices follow the process for drafting, reviewing, and approving directives.
- (5) Ensure all new directives are posted on the FCC intranet and internet, except for directives requiring special handling because of their sensitive content.
- (6) Administer the coordination of directives with bureaus and offices, as well as with the FCC chapter of the National Treasury Employees Union when the new or revised directive involves changes to employee working conditions.
- (7) Ensure that all directives are reviewed annually by the issuing bureau or office to ensure that they remain applicable and accurately represent current agency policies and procedures.
- (8) Have the authority to immediately remove from the internet or intranet any directive for security or legal reasons or because of incorrect content. The Office of General Counsel shall make a final determination to permanently remove content for legal reasons.
- (9) Issue changes to this directive that are necessary to implement and manage the FCC's directive management program.

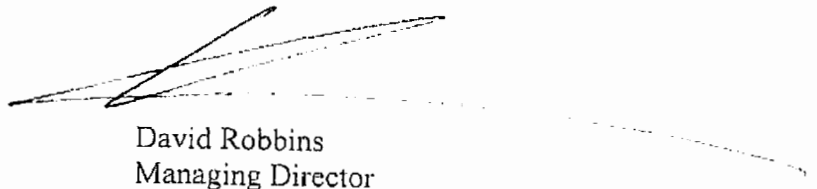
C. The Office of General Counsel. The Office of General Counsel is responsible for reviewing all new and revised directives for legal sufficiency.

D. The Office of Legislative Affairs. The Office of Legislative Affairs is responsible for notifying the appropriate originating bureaus and offices of relevant changes in legislation that may impact programs and require new or revised FCC directives.

E. Bureau and Office Chiefs. Bureau and office chiefs shall:

- (1) Establish necessary internal procedures to administer the directives system, including an internal checkpoint to review internal directives and handbooks for content and accuracy.

- (2) Conduct annual reviews of directives and handbooks originating in or applying to their bureaus or offices to determine if such documents require revision or cancellation.
- (3) Ensure that directives and handbooks clearly document programs, policies, functions, and procedures for which the bureau or office is responsible.
- (4) Provide training to appropriate personnel to ensure that the procedures described in directives and handbooks are correctly followed.
- (5) Coordinate the draft directives and handbooks with all impacted organizations within the agency. Coordinating bureaus and offices shall comment promptly and confine their comments to their functional areas.
- (6) Attempt to resolve all comments before finalizing the directive.
- (7) Track the draft and final directive through the review and clearance process. The originating office or bureau shall indicate a contact point with the expertise and authority to discuss the draft directive with the Office of Managing Director and make any requested changes. The Managing Director may schedule a meeting with the office or bureau point of contact to discuss the draft before granting final approval. Draft handbooks do not need to be coordinated with the Office of Managing Director, and shall become effective upon final approval of the chief of the originating bureau or office.



David Robbins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Electronic Mail Records Retention	
	Directive Number: FCC INST 1115.1	Effective Date: January 2017

Purpose. This Directive establishes the policy and assigns responsibilities for the Federal Communications Commission (FCC or the Commission) regarding the retention of electronic mail messages (email).

Scope. This Directive applies to all Email Users in the FCC headquarters and field units. This policy will be effective upon approval by the National Archives and Records Administration (NARA) of the FCC's request to implement Capstone.

Authority. 44 U.S.C. §§ 3101, 3301, *et seq.*; Presidential and Federal Records Act Amendments of 2014, Pub. L. 113-187, 128 Stat. 2091; 36 C.F.R. § 1236.22; Presidential Memorandum, Managing Government Records, dated November 28, 2011; OMB Memorandum M-12-18, Managing Government Records, dated August 24, 2012; OMB Memorandum M-14-16, Guidance on Managing Email, dated September 15, 2014; NARA Bulletin 2013-02, Guidance on a New Approach to Managing Email Records, dated August 29, 2013; NARA Bulletin 2014-06, Guidance on Managing Email, dated September 15, 2014.

Effect on Other Directives. This Directive supplements FCCINST 1110.2, FCC Records Management Program (Effective Date July 1, 2015) and FCCINST 1111.1, FCC Vital Records Program (Effective Date February 20, 2013) (together, referred to here as the "FCC Records Management Directives"). Unless specifically noted here, nothing in this Directive alters the existing FCC Records Management Directives.

Definitions

Accession: The transfer of physical and legal custody of permanent records to NARA.

Capstone: An email management approach developed by NARA that categorizes and schedules email based on the work and/or position of the Email User. This approach allows for the capture of all FCC emails (that are not Transitory Email Records or Non-Record Emails) and attachments as a records series from the accounts of officials at or near the top of an agency (or an organizational subunit) to be preserved as permanent. Under this approach, the emails of all other

Email Users (that are not Transitory Email Records or Non-Record Emails) are temporary records which are deleted after seven years.

Capstone Official: Unless otherwise noted by the Office of the General Counsel, FCC Capstone Officials are defined to include the Chairman, Commissioners, their advisors and confidential assistants, and any staff detailed as an advisor or confidential assistant to the Office of a Chairman or Commissioner for a period longer than 60 days; the Chief of any Bureau or Office as defined in section 0.5 of the Commission's rules, including Acting Chiefs serving longer than 60 days; any leaders appointed by the Chairman of any mission-centric task force, panel, or other temporary group¹; and any other positions identified on applicable records retention schedules as Capstone Officials. Capstone Officials shall also be defined to include the Chief Information Officer, Chief Financial Officer, and Chief Human Capital Officer of the FCC, as well as any other position designated by the Managing Director.

Culling: The process of removing or deleting Non-Record Emails and Transitory Email Records through manual and/or automated means. This may include, for example, deleting Non-Record Emails (such as spam or personal email) and Transitory Email Records that are no longer needed.

Email User: An employee, contractor, volunteer, intern, or any other person who uses the FCC email system.

Federal Records: All information, regardless of medium or format, made or received by the FCC under Federal law or in connection with the transaction of public business, either preserved or appropriate for preservation because of their administrative, legal, fiscal or informative value.

Non-Record Email: Non-record emails are those emails that do not meet the criteria of a federal record. Examples of emails that are typically non-record include, but are not limited to:

- Emails where no action is called for or taken or that are maintained solely for reference or convenience (for example, downloaded legal opinions or resource articles);
- Announcement of events;
- Trade journals and other publications;
- Mass informational emails (e.g., Monthly Health and Wellness Newsletter);
- Subparts and duplicates of email threads;
- News clips;
- Read or Delivery Receipts (automated reply email delivered to the sender when an email is delivered or opened by the recipient indicating the date and time the email is delivered or opened);
- Benefits Department communications;
- Learning Management communications;
- Spam; and

¹ See NARA's Record Schedule for Capstone Transmittal 26, p. 111 (providing that the heads of "mission-centric" task forces should be included as Capstone officials). In determining whether a task force, panel, or other temporary group is mission-centric, the Managing Director will consider such factors as whether (i) Congress required its creation under law; (ii) the agency announced its establishment publicly; and (iii) it engages with outside parties.

- Personal email.

Transitory Email Record: Email records of short-term (180 days or less) interest that have minimal or no documentary or evidentiary value. Transitory Email Records may be destroyed immediately, or when no longer needed for reference, or according to a predetermined time period or business rule.

Included in Transitory Email Records are such records as:

- Originating office copies of letters of transmittal that do not add any information to that contained in the transmitted material, and receiving office copy if filed separately from transmitted material;
- Quasi-official notices including memoranda and other records that do not serve as the basis of official actions, such as notices of holidays or charity and welfare fund appeals, bond campaigns, and similar records;
- Records documenting routine activities containing no substantive information, such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling related activities; and
- Suspense and tickler files or "to-do" and task lists that serve as a reminder that an action is required on a given date or that a reply to action is expected.

I. Policy

FCC Email Users routinely create, send, and receive electronic mail messages (email, email messages, or emails) to communicate information related to the mission or administrative matters of the Commission.² Emails (including their associated attachments) that contain content qualifying as federal records must be retained in electronic systems that provide the capability to identify, retrieve, and retain the records for as long as they are needed for statutory, regulatory, and business purposes in accordance with recordkeeping requirements for retention and disposition. This Directive provides guidance on the retention and deletion of FCC emails.

A. Treatment of Emails Generally

The incoming and outgoing emails of all Email Users will be available to the users in their electronic mailboxes for a period of time set by the Chief Information Officer (CIO). After the period of time has elapsed, the remaining emails will be archived. All emails of Capstone Officials that have not been culled will be accessioned to NARA after 15 years. The emails of all other Email Users will be archived and deleted after seven years.

If an Email User other than a Capstone Official sends or receives an email of lasting historical value that is not otherwise retained by a Capstone Official, the Email User will manually designate the email for permanent retention. Email Users sending or receiving a large number of such records should contact the Managing Director to determine if their position should be designated as a Capstone Official.

² The FCC permits staff, on a very limited basis, to use email for personal communication as long as it is within the *de minimis* use policy limitations found in the *FCC Cyber Security Policy* (version 3.6, effective May 2015).

B. Culling

The email of all Capstone Officials will be culled on a regular or routine basis to remove emails that are suitable for disposal prior to the transfer of those permanent records to the National Archives. This includes Transitory Email and Non-Record Emails, including personal emails.

C. Emails Subject to Preservation Holds

Email Users will retain any emails, regardless of its record status, as soon as the email becomes subject to a legal requirement to preserve or retain the email until the obligation to preserve ends. These preservation holds include, but are not limited to, emails subject to a Freedom of Information Act (FOIA) request, a Congressional records request, or a litigation hold. Once the preservation hold ends, the emails may be disposed of consistent with this directive.

D. Personal Email Accounts

In general, Email Users should not create or send record emails or attachments using non-official email accounts. However, should circumstances require the use of a personal account to conduct FCC business, the Email User must ensure that the communicated information is fully captured in an FCC recordkeeping system within 20 days, consistent with federal law³. If sending the email from a non-official account, the Email User must copy his or her FCC email address as a recipient. If receiving a work-related email on a non-official email account, the Email User must forward the work-related email to his or her FCC email account. Once the Email User has ensured the capture of the email information in the FCC account, the Email User shall remove the record email from the non-official email account.

II. Responsibilities

A. The Managing Director shall:

Oversee management of the FCC records management program, including email records management.

Designate positions as Capstone Officials.

Maintain and publish for all Email Users the email records retention requirements.

With OGC, conduct annual training on email records retention and Culling for all Email Users, including Capstone Officials.

B. The Associate Managing Director, Performance Evaluation and Records Management (AMD-PERM) shall:

³ Presidential and Federal Records Act Amendments of 2014, Pub. L. 113-187, 128 Stat. 2091, §10(a)(2)

Maintain a list of positions at the FCC that are determined to be the applicable Capstone records retention positions and notify and annually inform the persons holding those positions of their status as Capstone Officials.

C. The Chief Human Capital Officer (CHCO) shall:

Maintain a list of names and dates of tenure of all the individuals who are determined to be Capstone Officials.

Provide to the CIO and AMD-PERM any changes to the names and tenure of the FCC's Capstone Officials.

Provide support for the development and implementation of email records retention training for all Email Users.

D. The Chief Information Officer (CIO) shall:

Provide tools and approaches to maintain email in accessible and usable formats for the required retention period.

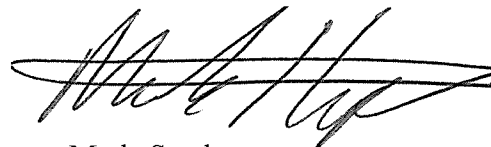
Ensure that processes and technology allow for retention of required email for periods identified herein; ensure removal of Non-Record Emails and Transitory Email Records through Culling; and ensure accession of email records to NARA.

Maintain a system or systems that will enable email records to be retained and stored in accordance with applicable records retention schedules and in approved email formats according to existing NARA transfer standards.

E. The General Counsel (OGC) shall:

Provide advice and assistance on all legal matters related to the administration of the FCC email records retention policy and practices.

With the Office of the Managing Director, conduct training on email records retention and Culling for all Email Users, including Capstone officials.

A handwritten signature in black ink, appearing to read 'Mark Stephens', with a stylized flourish extending from the end.

Mark Stephens
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Forms Management Program	
	Directive Number: FCCINST 116.1	Effective Date: August 2015

1. PURPOSE: This directive sets forth the Federal Communication Commission's ("Commission" or "FCC") policies, procedures, and responsibilities relating to the development and use of forms for official and authorized use in compliance with statutory and regulatory requirements.
2. SCOPE: The Commission's Forms Management program covers all the Commission's public-use forms and all internal-use forms used by more than one bureau or office. The policies and procedures set forth in this directive shall be followed by all managers and other staff with forms management responsibilities, including the authority to develop, edit, and administer new and revised forms.
3. AUTHORITIES:
 - a. The E-Government Act of 2002 (44 U.S.C. §3601)
 - b. Government Paperwork Elimination Act (44 U.S.C. §3504)
 - c. The Privacy Act of 1974 (5 U.S.C. §552a(e)(3))
 - d. The Paperwork Reduction Act (44 U.S.C. §§3501, *et seq.*) and the Office of Management and Budget's implementing regulations (5 C.F.R. §1320.3(c)(1); 5 C.F.R. §1320.3(f); 5 C.F.R. §1320.5(b)(2); and 5 C.F.R. §1320.5(h))
 - e. Section 508 of the Rehabilitation Act (29 U.S.C. 794d), *as amended by* the Workforce Investment Act of 1998 (P.L. 105-220)
 - f. 44 U.S.C. Chapters 31 and 33 and the implementing regulations regarding Records Management by Federal agencies found at 36 C.F.R. Parts 1220 through 1238.
4. POLICY:

It is FCC policy to:

- a. Establish and maintain an Agency-wide forms management program to increase the usefulness and effectiveness of forms in fulfilling the Commission's mission;
- b. Ensure all forms are directly linked to accomplishing a specific mission of the Commission and are necessary for the efficient and economical operation of the Commission;
- c. Eliminate unnecessary and duplicate forms and consolidate existing related forms;
- d. Increase the usefulness of forms through effective design and clear instructions to make it as easy as possible for respondents to provide the information requested; and
- e. Ensure that forms, to the maximum extent possible, make effective and efficient use of electronic technologies for the creation, collection, distribution, and use of these forms and to record, store, and disseminate information entered on those forms.

5. RESPONSIBILITIES:

- a. The Managing Director is responsible to ensure that procedures are developed and implemented to carry out the agency's Forms Management Program in an efficient, effective and economical manner as prescribed by Federal statute, regulation, and policy.
- b. The Associate Managing Director for Performance Evaluation and Records Management (PERM) is responsible for the administration of the Commission's Forms Management Program, including establishing overall policies, procedures and goals. This includes:
 1. Providing guidance to the Bureaus and Offices to ensure compliance with all applicable legislation, regulations, standards, and guidelines of forms management, analysis and design;
 2. Ensuring that the Commission's public-use forms meet the statutory and regulatory requirements associated with the Paperwork Reduction Act (as amended by the Government Paperwork Elimination Act) and the Privacy Act, which includes acting as the Commission's liaison to the Office of Management and Budget in regard to forms associated with Paperwork Reduction Act information collections;
 3. Maintaining a current inventory of all Commission internal-use forms and ensuring the Commission's inventory of public-use forms is kept current on the Internet;
 4. Reviewing new and revised forms to ensure personally identifiable information is only collected when there is a clear need to advance the mission of the Commission or to follow statutory or regulatory mandates;
 5. Coordinating the clearance of forms with OMB, GSA, or other government agencies


when necessary and as required;

- c. The Associate Managing Director for Administrative Operations (AO) is responsible for the procurement and printing of approved forms, ensuring that printing requests for forms are fulfilled in a timely manner and do not exceed the AO budget for forms.
- d. The Chief of each Bureau and Office is responsible for:
 - 1. Designating a representative to act as liaison to PERM on all matters concerning public-use (FCC) and internal-use ("A") forms for which the Bureau or Office is responsible;
 - 2. Ensuring all public- and internal-use forms are directly linked to accomplishing a specific mission of the Commission and can be demonstrably shown to be necessary for the efficient and economical operation of the Commission;
 - 3. When proposing any new form, providing a justification demonstrating why no existing form or data from existing forms could be used to accomplish the program mission;
 - 4. Conducting a review every three years to assess whether public- and internal-use forms the B/O originated still need to exist or if they can be eliminated or consolidated with other forms;
 - 5. Ensuring all forms are properly designed with clear instructions to make it as easy as possible for respondents to provide the information requested in the least amount of time;
 - 6. Ensuring that every form requesting Personally Identifiable Information (PII) contain the required Privacy Act disclosure notice;
 - 7. Ensuring all Commission public-use forms associated with information collections have the information required by 5 C.F.R. §§ 1320.6(a)(1), 1320.3(f) and 1320.5(b)(1) either on the form or in materials associated with the form;
 - 8. Ensuring that all Commission public-use forms are available via the Forms page on the Commission's web site, and that the forms linked to that page are the current versions;
 - 9. Ensuring forms (whether in paper or electronic form) are created, maintained, and disposed of in conformance with the Commission's Records Management Program;
 - 10. Ensuring PERM is promptly provided with a copy of every new or revised internal-use form, as well as notification when such forms are no longer used, so that a current inventory of such forms may be maintained; and

11. Responding promptly to any PERM notification regarding the need to replenish paper forms, and utilize Form A-100 to request printing from AO.

e. Forms Designers shall:

1. Design forms using software approved by the FCC and comply with applicable software end-user licensing agreements;
2. Incorporate plain language to the greatest extent possible in accordance with the OMB Final Guidance for the Plain Writing Act of 2010;
3. Ensure all requests to create, revise, and cancel forms containing PII contain the required Privacy Act statement; and
4. Ensure that forms are designed in an electronic format that conforms to applicable Section 508 Technical Standards to ensure ease of use by persons with disabilities, and promote electronic signature options in accordance with the Government Paperwork Elimination Act.


For Jon Wilkins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Federal Advisory Committees	
	Directive Number: FCCINST 1126.3	Effective Date: July 2016

1. Purpose - The purpose of this Directive is to set forth the Federal Communications Commission's (FCC's or Commission's) policy, administrative guidelines, and management controls relative to federal advisory committees.

2. Scope - This Directive applies to advisory committees established by the Commission under the rules of the FACA. The following types of groups are excluded from FACA and this instruction:
 - a. Groups assembled to solicit individual advice or exchange facts or information;

 - b. Committees composed wholly of federal, state, local, or tribal officials (intergovernmental committees) or wholly of federal government employees (intragovernmental committees);

 - c. Any local civic group whose primary function is that of rendering a public service with respect to any Commission program.

3. Authority - The Federal Advisory Committee Act (FACA or Act) as amended, 5 U.S.C., App 2; OMB Circular A-135, Management of Federal Advisory Committees; the General Services Administration's Federal Advisory Committee Management Final Rule, 41 CFR Parts 101-6 and 102-3; Executive Order 12024, Transfer of Certain Advisory Committee Functions; and Executive Order 12838, Termination and Limitation of Federal Advisory Committees.

4. Definitions
 - a. Advisory committee – Any committee, board, commission, council, conference, panel, task force, or other similar group, which is established by statute, by the President or by an agency official for the purpose of obtaining advice or recommendations on issues or policies within the

scope of an agency official's responsibilities.

- b. Committee Management Officer (CMO) - The individual designated by the agency head to implement the provisions of the FACA and any delegated responsibilities of the agency head under the FACA.
 - c. Designated Federal Officer (DFO) - An individual designated by the agency head, for each advisory committee for which the agency head is responsible, to implement the provisions of the FACA for that advisory committee under the control and supervision of the CMO.
 - d. Subcommittee - A group, generally not subject to FACA, that reports to the advisory committee and not directly to a federal officer or agency, whether or not its members are drawn in whole or in part from the parent advisory committee.
5. Policy - An advisory committee may be established only if it is essential to the conduct of agency business and if the information to be obtained from the committee's work is not already available through another advisory committee or source within the federal government. The advisory committee's recommendations will provide an important additional perspective affecting agency policy or operations. In accordance with FACA, an advisory committee is chartered for a two-year term. It will automatically terminate at that time unless the FCC Chairman authorizes the committee for another two year term, or the Chairman terminates the committee prior to expiration of its current charter.
6. Responsibilities:
- a. FCC Chairman - The Chairman will:
 - (1) Establish federal advisory committees as necessary to provide information and recommendations on telecommunications policy matters.
 - (2) Designate a CMO to oversee federal advisory committees under FCC sponsorship.
 - (3) Appoint a DFO for each committee established to serve as administrator for the committee.
 - (4) As a committee's charter expires, determine the need to continue the existing committee and approve its renewal.
 - (5) Appoint members of each federal advisory committee under FCC sponsorship as well as a committee chair.
 - b. Managing Director - The Managing Director will:
 - (1) Establish uniform administrative guidelines and management controls for all advisory committees consistent with FACA and implementing directives.
 - c. Committee Management Officer - The CMO will:
 - (1) Oversee all aspects of the FCC's Federal Advisory Committee program.

- (2) Approve all actions concerning the establishment, renewal, and termination of FCC advisory committees.
 - (3) Approve and certify the FCC's Annual Comprehensive Review of the agency's advisory committees chartered under FACA.
 - (4) Delegate responsibility for administering the Federal Advisory Committee program to the Associate Managing Director/PERM.
- d. Associate Managing Director/PERM (AMD-PERM) - The AMD-PERM will:
- (1) Recommend revisions, as necessary, to the administrative guidelines and management controls for committees established by the Commission and make the necessary revisions to keep this directive current with guidelines issued by the General Services Administration (GSA).
 - (2) Serve as a resource for the Commission and staff on questions concerning the application and administration of FACA.
 - (3) Advise the DFO of the termination date of a committee 60 days in advance of such date.
 - (4) Review and consult with committee DFOs to complete the FCC's Annual Comprehensive Review of the agency's advisory committees chartered under FACA.
- e. Bureau and Office Chiefs Bureau and Office Chiefs will:
- (1) Recommend to the FCC Chairman the need to establish or renew an advisory committee and furnish to the Chairman information which will provide a basis for approving the recommendation.
 - (2) Recommend to the Chairman an FCC employee to serve as DFO for a committee and, if necessary, recommend an alternate DFO.
- f. Designated Federal Officer The DFO or alternate will:
- (1) Approve all advisory committee meetings and subcommittee meetings;
 - (2) Approve the agenda for all meetings;
 - (3) Attend all meetings of the committee or any subcommittees;
 - (4) Adjourn any meeting whenever adjournment is determined to be in the public interest;
 - (5) Chair a committee meeting when so directed by the FCC Chairman.
 - (6) Maintain for his/her committee a complete set of charters, membership lists, minutes or reports from the committee, and records which fully disclose the disposition of funds, if any, at the disposal of each committee.
 - (7) Maintain a committee website that links from the FCC's website. The website will contain, at a minimum, the committee's current charter; list of members; list of subcommittees; reports and recommendations produced by the full committee; and meeting minutes, transcripts, and/or recorded webcasts of committee meetings.
 - (8) Review (subject to coordination with the Chairman, as appropriate) appointment of members to any working groups.

- g. General Counsel. The General Counsel will:
- (1) Provide advice to the Chairman, CMO and DFOs concerning requirements of FACA and GSA's regulations implementing FACA.
 - (2) Review proposed members of new and renewed federal advisory committees to ensure no conflicts of interest exist and that members are properly appointed either in a representative or individual capacity.

7. Procedures

a. Establishing a Committee

- (1) A request to establish a committee shall be submitted to the CMO from the Bureau or Office Chief whose organization has substantive responsibility for the subject matter of the committee. The request will include evidence of Chairman's Office approval to establish the committee, a draft charter for the committee and a Membership Balance Plan as required by GSA. These documents should be submitted at least 60 days prior to the date the committee would begin operations.
- (2) The committee charter will follow the format and contain the content found in GSA Guidance Document "Preparing Federal Advisory Committee Charters", dated November 2, 2011.
- (3) The Membership Balance Plan will follow the format and contain the elements found in GSA Guidance Document "Federal Advisory Committee Membership Balance Plan", dated January 2011.
- (4) Upon approval by the CMO to establish a committee, AMD/PERM will transmit to the GSA Committee Management Secretariat a request to establish a new federal advisory committee, including the proposed charter and Membership Balance Plan. GSA requests 15 calendar days for review, consultation, and concurrence with the request.
- (5) When the GSA Committee Management Secretariat has advised the FCC of its concurrence with the establishment of the committee, the DFO for the committee will publish a Notice of Establishment of Committee in the *Federal Register* at least 15 calendar days before the committee charter is filed. The Notice advises the public of the establishment of the committee, certifies that creation of the committee is in the public interest, and sets forth the nature and purpose of the committee. At the discretion of the DFO, a press release may be issued after publication of the notice in the *Federal Register* announcing establishment of the committee. This release may also be used to solicit nominations for committee members.
- (6) Fifteen days after the notice of establishment is published, AMD/PERM will file copies of the charter with a cover letter from the CMO to the Chair and Ranking Member of the FCC's Authorization and Appropriations Committees and Subcommittees, to the Library of Congress, and to the GSA Committee Management Secretariat. The date of this letter becomes the effective date on which the federal

advisory committee may commence operations. No committee shall meet to conduct any business or take action until a charter is filed.

b. Renewal of a Committee

- (1) Sixty days in advance of the termination date of a committee, AMD/PERM will advise the DFO of the upcoming termination date and request a decision concerning whether or not to renew the committee's charter.
- (2) If a committee has not completed its work and there is need to continue its existence, and the committee's DFO has obtained approval from the Chairman's Office to renew the committee, the DFO will request that the CMO seek GSA approval for renewal. This request will be accompanied by a copy of the committee's charter and Membership Balance Plan including any applicable edits since the previous charter and Membership Balance Plan.
- (3) AMD/ PERM will transmit to the GSA Committee Management Secretariat a request to renew the committee, including a revised charter and Membership Balance Plan. GSA requests 15 calendar days for review, consultation, and concurrence with the request.
- (4) When the GSA Committee Management Secretariat has advised the FCC of its concurrence with the renewal of the committee, AMD/PERM will file copies of the charter with a cover letter from the CMO to the Chair and Ranking Member of the FCC's Authorization and Appropriations Committees and Subcommittees, to the Library of Congress, and to the GSA Committee Management Secretariat. This becomes the effective date of the new charter and the date upon which the committee is officially renewed. The term of the renewed committee is two years from the filing date of the charter.
- (5) On or shortly after the effective date of renewal, the DFO for the committee will publish in the *Federal Register* a notice which advises of the renewal of the committee. No prior *Federal Register* notification is required.
- (6) At the discretion of the DFO, a press release may be issued announcing renewal of the committee. This release may also be used to solicit nominations for committee members.

c. Termination of a Committee – At the discretion of the FCC Chairman, a committee may be terminated at any time during the term of its charter. AMD/PERM will notify the GSA Committee Secretariat and request its concurrence to terminate. Otherwise a committee shall terminate when its charter expires and renewal of the committee is not requested by the FCC.

d. Selection of Members

- (1) The membership of each parent advisory committee shall be fairly balanced in terms of the points of view represented and the committee's function.

- (2) There shall be no discrimination in the selection of members on the basis of race, color, national origin, religion or gender.
 - (3) Appropriate safeguards shall be included to assure that the committee's advice and recommendations will not be inappropriately influenced by any special interest.
 - (4) Federally registered lobbyists shall not be appointed to serve as members of any advisory committee (or any working group) in an individual capacity, e.g. as Special Governmental Employees, although such individuals may be appointed to serve as members in a representative capacity.
- e. Subcommittees - The requirements of FACA and GSA's regulations concerning federal advisory committees do not apply to subcommittees that report to a parent advisory committee and not directly to the FCC or its staff. However, as with the selection of members of the advisory committee, the membership of each subcommittee shall be fairly balanced in terms of the points of view represented, and all meetings shall be approved in advance and called by the DFO or a designated alternate. The membership of a subcommittee shall be less than a quorum of the membership of the parent advisory committee.
- f. Meetings - The following requirements govern the preparation for and conduct of committee meetings:
 - (1) No committee will hold any meetings except at the call or with the advance approval of the DFO.
 - (2) Each meeting of a committee shall be conducted in accordance with an agenda approved by the DFO. The agenda shall list the matters to be considered at the meeting and shall indicate whether any part of the meeting is concerned with matters that are within the exemptions of the Government in the Sunshine Act, 5 USC 552b(c).
 - (3) No committee will conduct any meeting in the absence of the DFO or his/her designated alternate.
 - (4) Any federal advisory committee meeting must be announced in the *Federal Register* at least 15 days prior to the date of the meeting. The DFO is responsible for placing this notice in the *Federal Register* in a timely manner. The notice should contain:
 - (a) the name of the committee,
 - (b) the time and place of the meeting,
 - (c) purpose of the meeting and a summary of the agenda,
 - (d) information as to whether the meeting is open to the public or closed (if the meeting is closed state the reasons why, citing the specific exemptions in the Government in the Sunshine Act, 5 USC 552b(c) as the basis for closure),
 - (e) the name and telephone number of the DFO or other agency official who may be contacted for additional information concerning the meeting.

- (5) In exceptional circumstances, the FCC may give less than 15 calendar days notice. The circumstances must be included in the notice, and the Office of General Counsel (OGC) must give approval for publication of such notice
- (6) Other means of informing the public of an upcoming meeting, such as press releases and announcements on the committee's website, should be utilized to the extent practicable.

g. Public Participation - Each advisory committee meeting shall be open to the public except as described in Section 7h below and shall be subject to the following:

- (1) The meeting shall be held at a reasonable time and at a place that is accessible to the public;
- (2) The meeting room shall be of reasonable size, considering the size of the committee, expected public attendance and resources available to the committee and the Commission. Any meeting conducted via webcast meets the requirements of (1) and (2) of this section;
- (3) Any member of the public can file a written statement before or after the meeting;
- (4) Interested persons may be permitted by the committee or its chairman to present oral statements to the extent that time available for the meeting permits and must be in accordance with existing committee procedures;
- (5) Participation other than by presentation of oral or written statements by members of the public in committee meetings or questioning of committee members shall not be permitted except in accordance with established committee procedures.

h. Closed Meetings - Entire committee meetings or portions thereof may be closed to the public if the expressed purpose of the meeting will be to discuss subject matter which is within the exemptions contained in the Government in the Sunshine Act (5 USC 552b).

- (1) Closure of a meeting or portions of a meeting requires that the General Counsel and Chairman have determined that such closure is permissible under subsection (c) of section 552b of title 5, USC. This determination should be made in writing with an explanation of the reasons for closing the meeting. Notices of the meeting shall state whether any part of the meeting will be closed and state the reasons why. Meetings may be closed if they are likely to:
 - (a) disclose matters that are specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign policy and are in fact properly classified pursuant to such Executive order;
 - (b) disclose matters specifically exempted from disclosure by statute (other than 5 USC 552), provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria

for withholding or refers to particular types of matters to be withheld;

- (c) disclose trade secrets and commercial or financial information obtained from a person that is considered privileged or confidential;
 - (d) involve accusing any person of a crime, or formally censoring any person;
 - (e) disclose information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy;
 - (f) disclose investigatory records compiled for law enforcement purposes, or information which if written would be contained in such records, but only to the extent that the production of such records or information would interfere with enforcement proceedings; deprive a person of a right to a fair trial or an impartial adjudication; constitute an unwarranted invasion of personal privacy; disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source; disclose investigative techniques and procedures; or endanger the life or physical safety of law enforcement personnel;
 - (g) disclose information, the premature disclosure of which would be likely to significantly frustrate implementation of a proposed agency action, except in any instance where the agency has already disclosed to the public the content or nature of the proposed action, or where the agency is required by law to make such disclosure on its own initiative prior to taking final action on such proposal.
- (2) A committee member or DFO seeking to close a meeting (or portion thereof) must notify the CMO in writing at least 30 days before the date of meeting of its reasons for desiring to close the meeting. The CMO will immediately refer the matter to the Office of General Counsel and to the Chairman's office for review and a determination of whether closure is appropriate.
 - (3) When a meeting (or portion) is closed, members of the committee shall not disclose the matters discussed, except with other members of the committee, the staff of the committee, or FCC employees.

- i. Minutes - Detailed minutes shall be kept of each committee meeting. The committee chairperson may designate a member or a person who is not a member to take the minutes. The committee chairperson, or if unable to attend, his delegate, shall certify to the accuracy of the minutes. At a minimum, the minutes shall contain:

- (1) the time, date, and place of the meeting;

- (2) a list of committee members and FCC employees present, along with the names of members of the public who presented oral or written statements;
- (3) a complete summary of matters discussed and conclusions reached;
- (4) copies of all reports issued or recommendations approved by the committee.

j. Records

- (1) Subject to paragraph (2), each committee shall make its records, reports and other documents available on the committee's website for public inspection and copying, except access may be restricted on the basis of the exemptions contained in the Freedom of Information Act (FOIA), as amended, if there is a reasonable expectation that the records sought fall within the exemptions contained in section 552(b) of FOIA. When the only basis for denying access to a document is exemption (5), the CMO must make a positive determination that such a denial is essential to protect the free expression of internal views and to avoid interference with agency or advisory committee operations. This determination shall be reviewed and approved by the OGC.
- (2) Access shall be only to records which relate directly to an open meeting or open portion of a meeting where parts of the meeting were closed. A copy of the determination to close the meeting shall be made available to the public on request.
- (3) Committee records shall be available for public inspection until the committee ceases to exist. Requests for access to records not available on the committee's website should be directed to that committee's DFO.
- (4) Any person whose request for access to committee records has been denied can request administrative review in accordance with 0.461(i) of the Commission's Rules.
- (5) Substantive committee records are considered permanent Federal records and will be preserved and accessioned in accordance with General Records Schedule 6.2: Federal Advisory Committee Records.

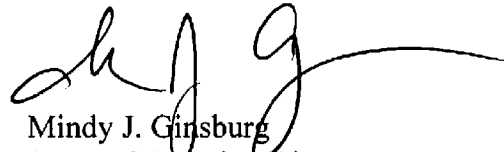
k. Administrative Requirements

- (1) Each Bureau or Office responsible for a committee shall provide the necessary support services to the committee. It may include in its budget submission a separate item for operation of committees.
- (2) The DFO is responsible for maintaining financial records of expenditures made to facilitate the legitimate activities of their committee.

l. Annual Comprehensive Review

- (1) The FCC will report to GSA on an annual basis, providing information on each federal advisory committee covered by FACA which is in existence during any part of a fiscal year.

- (2) DFOs will provide required information concerning their committee, using a government-wide system that GSA maintains.
- (3) The AMD-PERM and CMO will review the information for each committee and the CMO will certify to GSA that it is correct. This certification must be completed shortly after completion of a fiscal year by a deadline established by GSA.



Mindy J. Ginsburg
Deputy Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Information Security Program	
	Directive Number: FCCINST 1131.2	Effective Date: June 7, 2013

1. **PURPOSE:** This directive establishes the policy for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information requiring protection in the interests of national security. It primarily pertains to classified national security information, now known as classified information, but also addresses Controlled Unclassified Information (CUI) as outlined in E.O. 13556. The Federal Communications Commission (FCC) Information Security Manual contains the minimum standards for the protection of classified information and material. Such standards may be enhanced but never lessened as a commission option. This manual also provides guidance on the proper handling of sensitive unclassified material.
2. **SCOPE:** This directive applies to all FCC employees at headquarters and field units.
3. **AUTHORITY:** The statutory authority for this program is derived from Executive Order 13526, "Classified National Security Information," and 32 C.F.R., Part 2001, Title 18 of the United States Code, and guidance from the Office of Management and Budget and the National Security Council.
4. **POLICY:**
 - A. All FCC personnel, regardless of position, have a personal and official responsibility for the proper safeguarding and protection of the information to which they have access, particularly classified information.
 - B. Information will be categorized as classified or protected as sensitive only when it is in the interest of national security, and downgraded or declassified when it is determined that the information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than is currently required.
 - C. Information and material classified under this regulation will be afforded a level of protection against unauthorized disclosure commensurate with the level of classification or sensitivity assigned. Responsible officials will ensure that classified and sensitive information and materials are adequately protected from compromise.

D. Access to classified information is authorized only to the following personnel:

- (1) Persons with the appropriate need-to-know in order to perform a lawful and authorized governmental function;
- (2) Persons who have been granted a security clearance and access authorization at the appropriate level of clearance.
- (3) Persons who have executed an appropriate non-disclosure agreement. The FCC Personal Security and Suitability Manual contains policy on the personnel security clearance program. The holder, not the potential receiver of the information, determines the need-to-know and is responsible for verifying the clearance and access authorization of the potential receiver. No person will be granted access to classified information solely by virtue of their position.

E. Classified and sensitive information will be maintained only when necessary for the operation of the organization or when law, regulation, or records management policy requires its retention.

5. RESPONSIBILITIES:

A. FCC Chairman. The FCC Chairman shall

- (1) appoint a senior agency official to be responsible for direction and administration of the program within the FCC. This position will be the Security Officer for the FCC and hold the position title of Manager, Security Operations.
- (2) commit necessary resources to the effective implementation of the information security program.

B. Managing Director. The Managing Director will

- (1) designate a Commission Security Officer (CSO) by written appointment. The CSO will be of sufficient grade to effectively discharge assigned duties and responsibilities. The CSO will have direct access to the Managing Director and the FCC Chairman on matters affecting the information security program.
- (2) ensure adequate funding and resources are available to allow security management personnel to manage and administer applicable information security program requirements.
- (3) ensure the CSO is afforded security training consistent to the duties assigned.

C. Commission Security Officer. The CSO is the principal advisor on information security in the commission and is responsible to the OMD and Chairman for management of the program. The CSO will

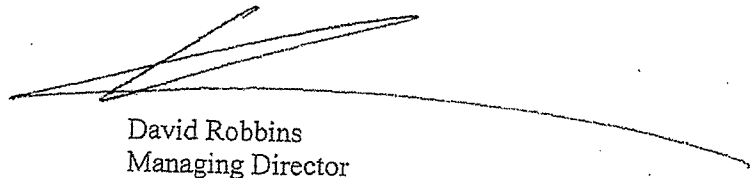
- (1) advise and represent the Managing Director and the FCC Chairman on matters related to the classification, downgrading, declassification, and safeguarding of national security information.
 - (2) establish written information security policies, procedures, and an effective information security education program.
 - (3) initiate and supervise measures or instructions necessary to ensure continual control of classified and sensitive information and materials.
 - (4) ensure that persons requiring access to classified information are properly cleared. The clearance status of each individual must be recorded and accessible for verification.
 - (5) review the effectiveness of the information security program in FCC bureaus and offices.
 - (6) ensure the prompt and complete reporting of security incidents, violations, and compromises, related to classified and sensitive information, as directed herein.
 - (7) ensure prompt reporting of credible derogatory information on assigned/attached personnel, to include recommendations for or against continued access.
 - (8) advise and assist officials on classification problems and the development of classification guidance.
 - (9) ensure that classification guides for classified plans, programs, and projects are properly prepared, distributed, and maintained.
 - (10) conduct a periodic review of classifications to ensure that classification decisions are proper.
 - (11) consistent with operational and statutory requirements, review all classified and sensitive documents in coordination with the FCC Records Management Officer. Continually reduce, by declassification, destruction, or retirement, unneeded classified and sensitive material.
 - (12) supervise or conduct security inspections and spot checks and notify the Managing Director regarding compliance with security regulations and directives.
 - (13) ensure that investigations and reporting of security violations is completed, including compromises or other threats to the safeguarding of classified and
-

sensitive information. Recommend corrective actions that should be taken concerning security violations.

- (14) ensure proposed public releases on classified and sensitive programs be reviewed to preclude the release of classified information or other sensitive unclassified information covered under the Freedom of Information Act (FOIA).
- (15) establish and maintain visit control procedures in cases in which visitors are authorized access to classified information.
- (16) issue contingency plans for classified and sensitive information and material and, where necessary, for the safeguarding of classified and sensitive information and material.

D. Bureau and Office Chiefs. Chiefs of FCC Bureaus and Offices will

- (1) ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, including sensitive information, for which they have a need-to-know.
- (2) ensure subordinate personnel are trained in, understand, and follow the requirements of this directive and Commission policy and procedures concerning the information security program.
- (3) ensure personnel follow procedures necessary to allow the continuous safeguarding and control of classified and sensitive information.



David Robbins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Insider Threat Program	
	Directive Number: FCCINST 1133.1	Effective Date: August 5, 2016

TO: All Employees

SUBJECT: Compliance with the FCC Insider Threat Program

Purpose

This directive establishes policy and assigns responsibilities for the Federal Communications Commission (FCC) regarding carrying out the requirements of the National Insider Threat Program. This Directive also authorizes issuance of the FCC *Insider Threat Implementation Plan (InThIP)* containing policies, procedures, roles, responsibilities, and information requirements for implementing the FCC Insider Threat Program. The FCC *InThIP* will be updated, as necessary, to reflect changes in law, regulation, or Presidential guidance or Executive Order. The FCC *InThIP* will be protected as Controlled Unclassified Information (CUI), and will be available only to the Managing Director (MD), the Senior Agency Official (SAO), Security Operations Center (SOC), and members of the Insider Threat Working Group (ITWG) on the Insider Threat electronic "Hub."

Scope

This Directive applies to all FCC Bureaus and Offices, and as well as Staff who hold any level of a National Security Clearance sponsored by the FCC, including Federal employees, contractors, temporary staff, interns, and volunteers.

Authorities

This Directive is published in accordance with guidance contained in Executive Order 13587 of October 7, 2011, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. The Executive Order establishes the requirement for federal agencies to develop, implement, and maintain an Insider Threat Program through the National Insider Threat Task Force (NITTF) which is co-chaired by the Attorney General and the Director of National Intelligence.

Other authoritative references as follows: White House Memorandum of November 21, 2012, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*; Executive Order 13526 of December 29, 2009, *Classified National Security Information*; White House Memorandum of August 23, 1996, *Early Detection of Espionage and Other Intelligence Activities*

Through Identification and Referral of Anomalies; Section 811 of the Intelligence Authorization Act of October 14, 1994; Presidential Decision Directive/NSC-12 of August 5, 1993, *Security Awareness and Reporting of Foreign Contacts*; Executive Order 12333 of December 4, 1981 (Amended), United States Intelligence Activities; Executive Order 10450 of April 27, 1953, *Security Requirements for Government Employment*. Other related authoritative FCC reference include FCC Directive FCCINST 1131.2 *FCC Information Security Program* effective June, 2013 and *FCC Information Security Manual* effective June, 2013.

Policy

An insider threat arises when a person with authorized access to classified U.S. Government resources, including personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. The FCC Insider Threat Program goal is to deter, detect, and mitigate actions by Staff who may represent a threat to national security. These threats encompass potential espionage, violent acts against the Government or the nation, and unauthorized disclosure of classified information including data available on interconnected United States Government computer networks and systems.

The FCC Insider Threat Program includes the capability to gather, integrate, and centrally analyze and respond to key insider threat-related information; monitor Staff use of classified information systems and material; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

Responsibilities

Listed below are the major responsibilities for the key positions that oversee the FCC Insider Threat Program. A complete list of roles, responsibilities, policies, procedures for carrying out the program and information regarding deterrence, detection, and mitigation of threats to national security are located in the FCC *InThIP* document.

A. The Managing Director (MD) shall:

1. Oversee the FCC Insider Threat Program and allocate adequate resources to carry out its implementation; and
2. Act as or appoint the Senior Agency Official for the FCC Insider Threat program;

B. The Senior Agency Official (SAO) for the FCC Insider Threat Program shall:

1. Ensure efficient and effective management, accountability, and day-to-day oversight of the FCC's Insider Threat Program, and;
2. Ensure the Chief Security Officer, Security Operations Center (SOC), Administrative Operations (AO), Office of the Managing Director (OMD) as the principal lead, carries out the responsibilities and functions of the FCC's Insider Threat Program.

C. The Chief Security Officer, SOC, as principal lead, shall:

1. Carry out the FCC Insider Threat program and make resource, policy, procedure, and process recommendations to the MD/SAO;

2. Serve as the FCC Insider Threat Program Manager (InThPM) and have the Deputy Chief Security Officer serve as the FCC Insider Threat Deputy Program Manager (InThDPM);
3. Serve as the Chair of the FCC Insider Threat Working Group (ITWG) and have the Deputy Security Officer serve as the Deputy Chair of the ITWG;
4. Ensure that the all aspects of FCC Directive FCCINST 1133.1, *Compliance with the FCC Insider Threat Program* and the *FCC InThIP* are carried out in accordance with Executive Order 13587 and NITTF guidance as well as other reference authorities listed above;
5. Seek support from owners of Classified networks, per Executive Order 13587 and NITTF, for the technical capability, subject to appropriate approvals, to monitor user activity on all Classified networks in order to detect activity indicative of insider threat behavior;
6. Develop a comprehensive process to gather, integrate, and centrally analyze and respond to counterintelligence, security, information assurance (information technology), human resources, law enforcement, and other relevant information indicative of a potential insider threat;
7. Implement policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel;
8. Maintain a file of non-disclosure agreements signed by all FCC cleared individuals acknowledging that they must adhere to all laws and regulations with respect to protecting Classified information;
9. Maintain a file of agreements signed by all FCC cleared individuals, acknowledging that they have no expectation of privacy with respect to their activity on any agency Classified network, to include portable electronic devices, and that such activity is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding;
10. Ensure that “banners” exist on FCC (subscriber) Classified networks that inform users that they have no expectation of privacy with respect to their activity on such networks, that their activity on such networks will be monitored to ensure that user activity is for lawful United States Government authorized purposes, and that misuse and/or compromise of Classified information can result in criminal, security, or administrative actions against the users;
11. Develop guidelines for B/Os to securely, discretely, and in a timely manner, provide the FCC InThPM/InThDPM upon request information necessary to identify, analyze, and resolve insider threat matters;
12. Establish a FCC Insider Threat Working Group (ITWG) comprised of appropriate staff to include but not limited to individuals from the Office of Managing Director’s front office, SOC, Human Resources Management, Information Technology Center, as well as individuals from the OGC and PSHSB. Upon FCC InThPM/InThDPM request, members of

the FCC ITWG will securely, discreetly, and in a timely manner, provide the FCC InThPM/InThDPM information necessary to identify, analyze, and resolve insider threat matters;

13. Ensure that FCC personnel assigned to the ITWG are fully trained in the following: the Insider Threat Program and applicable counterintelligence and security fundamentals; FCC procedures for conducting insider threat response actions; applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information; applicable civil liberties and privacy laws, regulations and policies; and in investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal or external entity;
14. Ensure FCC Insider Threat awareness training is provided and that training course completion is verified for all new cleared and non-cleared employees at entry-on-duty and for all cleared and non-cleared employees annually;
15. Ensure the FCC Insider Threat awareness training to all personnel annually addresses current and potential threats in the work and personal environment and shall include, at a minimum, the following topics: the importance of detecting insider threats and reporting suspicious activity to the InThPM/InThDPM and methodologies of adversaries to recruit trusted insiders and collect Classified information;
16. Establish a secure internal electronic FCC Insider Threat site (“Hub”) that is accessible to all FCC cleared individuals and the MD, SAO, SOC, and ITWG. The FCC Hub provides insider threat reference material, including indicators of insider threat behavior, training information, reporting requirements, policy, procedures, roles, responsibilities and a secure means of reporting to and reviewing matters of the Insider Threat Program. The electronic Hub is segmented and limits access to the *FCC InThIP* and specific insider threat information to only the MD, SAO, SOC, and ITWG as necessary. The InThPM/InThDPM is responsible for making all access decisions regarding insider threat information contained in the Hub;
17. Implement oversight mechanisms and/or procedures to ensure proper handling and use of records and data;
18. Limit access as necessary to such records and data to only those staff who require the information to perform their authorized FCC Insider Threat Program function;
19. Ensure adherence to guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587, and NITTF, and;
20. Produce an annual report to the MD, SAO, and NITTF’s Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to ensure compliance with the FCC and the National Insider Threat Program as prescribed by Executive Order 13587 and NITTF.

D. FCC Insider Threat Working Group (ITWG) shall:

1. Provide information to the FCC Chair and FCC Deputy Chair of the ITWG who also serve as the FCC InThPM/InThDPM;
2. Be fully trained in the following: the Insider Threat program and applicable counterintelligence and security fundamentals; FCC procedures for conducting insider threat response actions; applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information; applicable civil liberties and privacy laws, regulations and policies; and investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal or external entity;
3. Have appropriate access to the *FCC InThIP* and insider threat information available at the FCC Hub;
4. Upon FCC InThPM/InThDPM request, securely, discretely, and in a timely manner, provide the FCC InThPM/InThDPM information necessary to identify, analyze, and resolve insider threat matters.

E. FCC Bureaus and Offices shall:

1. Have access to Directive FCC INST 1133.1, *Compliance with the FCC Insider Threat Program* which describes, in general nature only, the policy and responsibilities of the FCC regarding carrying out the requirements of the National Insider Threat Program.
2. Upon FCC InThPM/InThDPM request, securely, discretely, and in a timely manner, provide the FCC InThPM/InThDPM information necessary to identify, analyze, and resolve insider threat matters, to the extent that the InThPM/InThDPM require information other than can be provided by the ITWG.

F. Classified Network Subscriber shall:

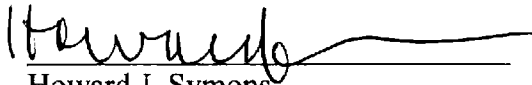
1. Seek support, per Executive Order 13587 and NITTF guidance, for the technical capability, subject to appropriate approvals, to monitor activity in order to detect insider threat behavior on classified computer systems.

G. Office of the General Counsel shall:

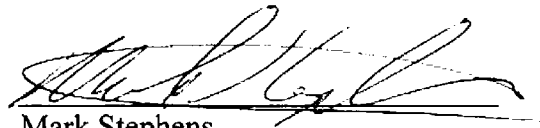
1. Advise and assist on all legal matters related to the administration of the FCC Insider Threat Program;
2. Oversee FCC Insider Threat Program compliance with applicable civil rights, civil liberties, and privacy requirements.

H. All FCC Cleared Individuals shall:

1. Report to the InThPM/InThDPM all contacts, activities, indicators, or behaviors that they observe or gain knowledge of that could adversely impact the responsible sharing and safeguarding of Classified information. A list of reportable contacts, activities, indicators, and behaviors as well as current information materials are available at the FCC Hub and is accessible by all FCC cleared individuals.



Howard J. Symons
General Counsel, FCC



Mark Stephens
Managing Director, FCC

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	FCC Personnel Suitability and Security Program	
	Directive Number FCCINST 1135.2	Effective Date August 2011

1. Purpose: This instruction establishes the policies and procedures of the Federal Communications Commission (FCC) Personnel Suitability and Security Program.
1. Cancellation: This directive replaces FCCINST 1135.1, FCC Personnel Suitability and Security Program Manual, dated August 2006.
2. Background: This directive and the accompanying manual provide guidance and an understanding of the responsibilities and duties of the FCC Personnel Suitability and Security program. The manual will be updated routinely as the security and suitability requirements affecting federal personnel and contractors change in response to new technologies and national policies. The most current information on personnel suitability and security requirements is available for review at the Security Operations Center (SOC).

The Federal Government mandates that all appointees, employees, and contractors be suitable for Federal employment. The Personnel Suitability and Security Manual contains the FCC's policy implementing those mandates. The manual provides guidance to the Personnel Suitability and Security Program as to position risk and sensitivity level designation, investigation requirements, and security/suitability adjudication for an individual's employment with the FCC. Under a Memorandum of Agreement with the U.S. Office of Personnel Management (OPM), OPM will conduct all background investigations requested by the FCC.

The FCC adjudicates an individual's employment suitability based on that individual's ability to obtain and maintain a national security clearance or suitability access based on the investigation's findings. Every appointment, including contractor positions, is subject to suitability and investigative processing. A smaller subset of individuals may also undergo further investigation related to obtaining higher-level security clearances. The purpose of this manual is to ensure individuals who have or could have access to either classified and/or sensitive/proprietary information receive fair, impartial, and equitable treatment in the processing and adjudication of their clearance or suitability determinations. The policies and procedures in this manual are in accordance with the FCC's responsibilities to protect both the public trust and promote the national security.

4. Scope and Applicability: This manual applies to: 1) all applicants, selectees, or appointees for temporary and/or permanent positions in either a single continuous or series of appointments; 2) all FCC employees (i.e., competitive, excepted, and Senior Executive

Service) in permanent positions who move to a position designated at a higher risk/sensitivity level; 3) all contractors, subcontractors, experts, consultants, or other persons whose services may be used under a full-time or part-time contract; and 4) all operating officials involved in identifying and designating position risk/sensitivity levels to include referrals of investigative information. All persons listed in categories 1) through 4) above will be referred to as "individuals" for all purposes concerning this manual's guidance unless otherwise noted.

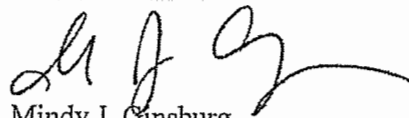
This manual is intended for use by officials involved in determining an individual's suitability for employment and/or security access eligibility, designating position risk/sensitivity levels, and evaluating, updating, and modifying position duties or descriptions. These officials include but are not limited to Bureau chiefs, Branch chiefs, Supervisors, Human Resource staff, and Personnel Security staff.

5. Authorities: The Managing Director (MD) under the requirements of Title 47, Subpart A, § 0.11, has the responsibility to plan and manage Commission activities related to personnel suitability and security and therefore, the authority to implement the FCC Personnel Suitability and Security Program.

The MD, or Deputy MD if so designated by the MD, shall be assisted by the Associate Managing Director for Human Resources Management (AMD-HRM) and the Associate Managing Director for Administrative Operations (AMD-AO) in managing and implementing the FCC Personnel Suitability and Security. The MD, in consultation with the AMD-HRM and the AMD-AO, has established the Security Operations Center (SOC) within the AMD-AO.

The MD appoints a Security Officer and Security Specialists to carry out the day-to-day duties and responsibilities of the FCC's Personnel Security and Suitability Program.

The statutory authorities guiding this program include: Executive Order (E.O.) 10450, and E.O. 10577 (as amended by E.O. 12107), E.O. 12829, E.O. 13526, E.O. 12968; Public Law 100-235, Computer Security Act of 1987; Chapter 73 of Title 5, U.S. Code, Government Organizations and Employees; Title 5 Code of Federal Regulations (CFR) 731, 732, and 736; OMB Circular A-130, Appendix III; the FBI's National Security Threat List and other OPM and Federal agency guidance.



Mindy J. Ginsburg
Deputy Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Monitoring and Recording of Telephone Conversations	
	Directive Number: FCCINST 1137.2	Effective Date: June 30, 2011

1. Purpose. Pursuant to Section 4(i) of the Communications Act of 1934, as amended, 47 U.S.C. § 154(i), this directive prescribes the policy applicable to the practice of monitoring or recording of telephone conversations by Commission personnel.
2. Supersession. FCC Directive FCCINST 1137.1, dated January 2000 is superseded.
3. Background. Numerous federal and state laws govern the interception of telephone and oral communications. The term “interception” is broadly defined and encompasses both the monitoring and recording of such communications. While some laws permit interception when only one party to the conversation consents, all laws permit interception when all parties to the conversation consent.
4. Definition. As used hereafter, the term “interception” includes the monitoring (listening-in) or recording of telephone or video conversations, including conversations held using a microphone, webcam, or similar device over the internet.
5. Policy.

The following points are FCC policy:

- (a) Except with the prior written approval by the General Counsel, and the exceptions stated in subsections (b) and (c) below, no telephone or video conversation by or to officials and employees of this agency shall be intercepted by any Commission personnel, unless:
 - (1) Such records will substantially contribute to the effective conduct of official business; and
 - (2) All parties remotely participating in the conversation have been informed at its outset that it will be monitored, transcribed, intercepted, or recorded, and they have consented to such actions prior to the conversation either orally or in writing, regardless of the purpose for which it is being recorded.

(b) With regard to public meetings, conferences, or other proceedings, notice is considered sufficient if included either: (i) in the public notice initially announcing the forum, or (ii) on the Commission's website, as part of the instructions on how individuals may participate or listen remotely to the public meeting, conference, or other proceeding.

(c) Approval by the General Counsel is not required for interceptions conducted or authorized by the Inspector General.

6. Responsibilities.

(a) The Commission has designated the General Counsel as the approving authority for any requests to intercept a telephone or video conversation by Commission personnel except as specified above.

(b) Bureau/Office Chiefs, except as specified above, will make an initial written request for authorization to engage in any interception for which consent of all parties will not be obtained.

(c) The General Counsel will make determinations on a case-by-case basis applying the applicable law in each instance. For each instance of approved interception, the General Counsel will submit to the requesting Bureau/Office detailed directions concerning methodology and recordkeeping.



Mindy J. Ginsburg
Deputy Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554	TITLE	
	Management of Nonpublic Information	
	Directive Number: FCC INST 1139.1	Effective Date: February 2015

TO: All Employees

SUBJECT: Management of Nonpublic Information

1. Purpose and Scope

The purpose of this directive is to establish policies and procedures for managing and safeguarding nonpublic information. The Commission has four general categories of information: (1) classified national security information; (2) sensitive but unclassified information having to do with homeland security, law enforcement, intelligence, defense, and foreign affairs; (3) nonpublic information; and (4) information routinely made available for public inspection.

This directive applies to all category 3 nonpublic information in all formats, including, but not limited to, paper, computer files, emails, diskettes, CD-ROMs, audio and video recordings, and oral communications. This directive DOES NOT apply to category 1 classified national security information and category 2 sensitive but unclassified information having to do with homeland security, law enforcement, intelligence, defense and foreign affairs. The policies and procedures for managing and safeguarding category 1 and 2 information can be found in the Information Security Manual (FCC Instruction 1131.2).

The Freedom of Information Act and the Privacy Act apply to all four categories of information and this directive neither negates nor supersedes the requirements of those statutes.

All employees are subject to the requirements outlined here. These requirements are also applicable to contractors as a term of their contract with the Commission.

2. Policy

Unauthorized disclosure of nonpublic information is prohibited by Section 19.735-203 of the Commission's rules and may result in disciplinary action. 47 C.F.R. Section 19.735-107. In the case of contractors, unauthorized disclosure may result in termination of the contract, replacement of a contract employee or other appropriate measures.

3. Background

Section 0.451 of the Commission's rules explains that records routinely available for public inspection are listed in Sections 0.453 and 0.455 of the Commission's rules and all other records are not routinely available for public inspection. Section 0.457 of the Commission's rules lists by category information the Commission has determined to withhold from public inspection. Section 0.457 explains, as appropriate, the legal and policy rational for withholding from public inspection each category of information listed in the rule.

4. Definitions

Nonpublic Information. Nonpublic information includes all information that (i) is NOT routinely available for public inspection and (ii) is NOT characterized as category 1 classified national security or category 2 sensitive but unclassified having to do with homeland security, law enforcement, intelligence, defense and foreign affairs. As defined below, there are two types of nonpublic information: "Highly Sensitive/Restricted" and "For-Internal Use Only."

(1) **Highly Sensitive/Restricted.** Information that is highly market-sensitive (*i.e.*, disclosure of which is likely substantially to affect the value of securities traded publicly or a company's market valuation); commercial or financial information the Commission considers confidential and highly sensitive, and any other material that is deemed highly sensitive, in the discretion of a Bureau/Office chief.

- a. For purposes of determining whether disclosure of information is likely substantially to affect the value of securities or market valuation, factors to consider include: the size of the transaction, in total dollar value or other objective measure (where applicable); the level of external interest; and/or whether the proceeding is likely to set a novel or important precedent.
- b. Bureau and Office Chiefs in exercising their discretion may conclude that particular types of proceedings are always deemed Highly Sensitive/Restricted. For example, agenda: and circulation enforcement cases are particularly sensitive because unauthorized disclosures of nonpublic information to a target of an enforcement

action or to a third party can have potentially severe consequences for the enforcement matter itself as well as for targets, other parties involved in investigations, the Commission as a whole, and individual employees at every level. As a result, to protect the identity of the target and the nature of the investigation against it until the Commission acts by taking public action, all circulation and agenda enforcement cases are deemed Highly Sensitive/Restricted.

(2) **For-Internal Use Only.** All nonpublic information that is NOT Highly Sensitive/Restricted.

5. Unauthorized Disclosure, Loss or Theft

Any unauthorized disclosure, loss, or theft of nonpublic information should be reported to the Bureau or Office Chief or the Inspector General.

6. Procedures for Handling Nonpublic Information

- a. **Determination of Category.** The Bureau or Office responsible for creating information or using information (in the case of material submitted to the agency) is responsible for determining into which category the information falls. This may be accomplished in consultation with the Office of General Counsel. Where more than one Bureau or Office is participating in a matter, the lead Bureau or Office (*i.e.*, the organization responsible for drafting a decision, preparing a report or audit, etc.) will make the determination. As noted above, all circulation and agenda enforcement cases are deemed Highly Sensitive/Restricted. Commercial or financial information for which a request for confidential treatment is pending may be accorded the protections set forth in this directive that are applicable to Highly Sensitive/Restricted information, in the discretion of the Bureau or Office handling the matter. Otherwise, until a determination is made, such material will be accorded confidential treatment, consistent with Section 0.459 of the Commission's rules.
- b. **Other Relevant Directives.** Guidance regarding maintaining and disposing of nonpublic information is also included in the following directives:
 - (1) FCC Cyber Security Program (FCC INST 1479.4)
 - (2) Records Management Program (FCC INST 1110.1)
 - (3) Freedom of Information Act (FOIA) Request (FCC INST 1179.2)
 - (4) Privacy Act Manual (FCC INST 1113.1)
- c. **Disposal.** Nonpublic information at the Commission's headquarters building must be disposed of in a locked document disposal bin. These bins are located throughout the Portals I and II buildings, including all copier rooms, front offices and Chairman/Commissioner' offices. Material at non-headquarters locations (for example, in field offices, Gettysburg, Laurel lab, etc.) should be disposed of in a

- manner that protects it from unauthorized public disclosure consistent with local practices.
- d. **Commission Agenda and Circulation Items/Cover Sheets.** Circulation and agenda items that are not categorized as Highly Sensitive/Restricted and that are distributed to any person or Bureau or Office must bear a cover sheet marked "For Internal Use Only/Nonpublic." These cover sheets are available from the Office of the Secretary to be used for open meeting items (blue) or circulation items (pink). This directive does not modify procedures for electronic distribution of agenda items set forth in the Agenda Handbook for items categorized as For Internal Use Only. Agenda items categorized as Highly Sensitive/Restricted shall be handled as specified below.
- e. **Special Procedures for Nonpublic Highly Sensitive/Restricted Information.** The following procedures apply only to Highly Sensitive/Restricted information:
 - (1) Each time a decision is made to designate a piece of nonpublic information as Highly Sensitive/Restricted, a primary contact must be designated by a Bureau or Office Chief or other senior official as having lead responsibility for the particular matter or item that is considered Highly Sensitive/Restricted. Where more than one Bureau or Office is participating in a matter, the primary contact will be designated by the Bureau or Office having lead responsibility for that matter. The lead Bureau or Office may also designate a back-up primary contact in the event that the primary contact is unavailable.
 - (2) Only staff directly responsible for handling the matter or those with a "need to know" may have access to Highly Sensitive/Restricted information. This requirement applies to both written and oral communications. The primary contact will monitor who has access to Highly Sensitive/Restricted information through means determined by the primary contact as appropriate to each specific situation.
 - (3) In no circumstances should Highly Sensitive/Restricted information be left in a place accessible to non-authorized personnel when not in use.
 - (4) Labeling, copying and dissemination.
 - a. Each page of Highly Sensitive/Restricted documents created by the agency should be labeled. For most documents, the label should denote that the document contains "NONPUBLIC, CONFIDENTIAL, HIGHLY SENSITIVE/RESTRICTED INFORMATION." Highly Sensitive/Restricted documents created by the Enforcement Bureau should be labeled "NONPUBLIC, CONFIDENTIAL, HIGHLY SENSITIVE LAW ENFORCEMENT INFORMATION."
 - b. Enforcement cases on circulation shall include a special notice at the top of the Cover Memo. This notice shall clearly denote that the case on circulation is an "Enforcement Case" and cite the Commission's

rules prohibiting the disclosure of nonpublic information. The notice shall be printed in red or other color to highlight the importance of protecting Highly Sensitive/Restricted nonpublic information in enforcement cases and shall include, at a minimum, the following text:

NONPUBLIC, CONFIDENTIAL, HIGHLY SENSITIVE
THIS IS AN ENFORCEMENT CASE.
UNAUTHORIZED DISCLOSURE IS PROHIBITED.

Enforcement investigations and actions are strictly confidential. All employees are prohibited from disclosing any information about an enforcement matter to any person outside the Commission, whether directly or indirectly. *See* 47 C.F.R. §§ 0.457, 0.459(d)(3), 19.735-203(a). Unauthorized disclosure of nonpublic information about enforcement matters subjects the Commission employee to possible disciplinary action pursuant to 47 C.F.R. § 19.735-107.

- c. Special care should be exercised when copies are made on shared printers and copying machines.
- d. Paper copies must be distributed in sealed envelopes labeled "Special Attention mail: To be opened by _____." These envelopes may be obtained from the Administrative Services Center (ASC). Labeled cover sheets, which are also available from the ASC, may be placed on top of the document as a further precaution.
- e. Copies should never be left in unsecured In-Boxes or on unattended desks or chairs.
- f. For electronic dissemination, the transmission should clearly note that the information is Highly Sensitive/Restricted and the information should only be transmitted under secure conditions to individuals with a need to know.
- g. Notwithstanding the Highly Sensitive/Restricted nature of all circulation and agenda enforcement cases, the Office of Inspector General may disclose information about an enforcement matter to another law enforcement agency as authorized by the Inspector General Act of 1978, as amended.

7. Training Program

Every new employee shall receive a brochure setting forth the policies in this directive during their new employee orientation.

8. Responsibilities


a. **Bureau and Office Chiefs (or their designees) shall:**

- (1) Appoint a primary contact and a back-up for each matter involving Highly Sensitive/Restricted information in which the Bureau or Office has lead responsibility.
- (2) Take reasonable measures to ensure compliance with nonpublic information management controls set forth herein.
- (3) Categorize information into levels of protection noted above, and determine who within the organization should have access to Highly Sensitive/Restricted material.
- (4) Advise OMD if additional computer or other security resources are needed to maintain security for Highly Sensitive/Restricted information.
- (5) Refer as appropriate alleged unauthorized disclosure, loss or theft to the Inspector General.
- (6) Seek appropriate authorization pursuant to Section 19.735.203 of the Commission's rules prior to disclosure of nonpublic information when appropriate.

b. **The Managing Director shall:**

Establish and disseminate policies and procedures to protect nonpublic information and ensure those policies are coordinated with all the information policies noted in this directive.

Provide material necessary to the implementation of this policy (document disposal bins, stamps, templates, envelopes, cover sheets, etc.).


Jon Wilkins
Managing Director

<p>FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554</p> <p>FCC DIRECTIVE</p>	Title	
	Forfeiture Tracking, Collections and Follow-up Systems	
	Directive Number FCC INST 1157.4	Effective Date April 2016

1. **PURPOSE**: This directive sets forth the Federal Communications Commission’s (“FCC” or “Commission”) policies, procedures, guidelines, and responsibilities relating to the FCC’s Civil Monetary Penalty (“CMP”) Program. It provides persons involved in recording, tracking, and reporting of the FCC’s forfeiture proceedings and payments with a summary of relevant Commission policies, procedures, and internal controls necessary to maintain accountability of receivables and administrative proceedings resulting in a CMP. The primary objectives are to:
 - a. Ensure timely and uniform recording, tracking and monitoring of forfeiture proceedings;
 - b. Ensure timely deposits in a U.S. Department of Treasury (“Treasury”) approved lockbox bank of remittances arising from forfeiture proceedings;
 - c. Ensure timely and accurate reporting to Bureaus and Offices (“B/Os”) of transactions and balances;
 - d. Ensure adequate internal controls including separation of duties;
 - e. Ensure that the FCC Office of General Counsel (“OGC”) refers to the U.S. Department of Justice (“DOJ”) forfeiture proceedings that meet DOJ acceptance standards in a timely manner; and
 - f. Maintain accountability of all forfeitures issued by the Commission.
2. **AUTHORITY**:
 - a. Telecommunications Rules and Regulations 47 C.F.R. §§0.111, 0.311, 0.314, 1.80, 1.1901.
 - b. Money and Finance 31 U.S.C. §§ 3701, 3711.
 - c. Money and Finance Treasury 31 C.F.R. §§ 285, 901-903.
 - d. Forfeitures 47 U.S.C. §§ 503, 504.
3. **SCOPE**: This directive applies to all B/Os of the Commission that issue, track, or enforce forfeitures, refer forfeitures to DOJ, or process remittances pertaining to forfeitures.

4. DEFINITIONS:

- a. Civil Monetary Penalty (CMP). A monetary penalty or forfeiture proposed, assessed or enforced by the Commission pursuant to Federal Law, including court ordered payments resulting from judicial enforcement of a Forfeiture Order.
- b. Consent Decree (CD). An agreement resolving an investigation or forfeiture proceeding pertaining to a violation of the Communications Act, a Commission rule, a Commission order, or a term or condition of a Commission authorization through a voluntary contribution to the Treasury and future administrative compliance.
- c. Debt. An amount of money, funds, or property that has been determined by an agency official to be due to the United States from any person, organization, or entity, except another Federal agency. "Claim" and "debt" include amounts due the United States from fees, penalties, damages, interest, taxes, and forfeitures issued after a Notice of Apparent Liability that have been partially paid or for which a court of competent jurisdiction has ordered payment and such order is final.
- d. Debt Collection Officer (DCO). The employee responsible for collecting outstanding debts or other amounts owed to the Commission. The DCO is a designated management official from within the Office of the Managing Director (OMD), Office of the Chief Financial Officer (OMD-FO). OMD-FO is responsible for administering the collection of the Commission's outstanding debts.
- e. Debt Collection Procedures. Procedures for debt collection that comply with 31 U.S.C., 47 C.F.R., and 31 C.F.R.
- f. Demand Letter. The initial step of debt collection procedures used by OMD-FO, in which OMD-FO sends a letter and invoice to the subject of the legally enforceable debt, demanding full payment of the debt by a certain date.
- g. Forfeiture Follow-up. Actions taken by OMD-FO to collect a forfeiture penalty after the amount has become a legally enforceable debt using debt collection procedures – issuance of a payment Demand Letter and invoice, permitting payment under the terms of an installment payment plan, or referral to Treasury for delinquent debt collection.
- h. Forfeiture Order (FO). An order issued by the Commission or by the Enforcement Bureau or Media Bureau under delegated authority assessing a monetary forfeiture for a violation of the Communications Act, a Commission rule, a Commission order, or a term or condition of a Commission authorization. An FO is not a legally enforceable debt until either a partial payment is made, or a court of competent jurisdiction has issued an order enforcing the forfeiture that is final.
- i. Notice of Apparent Liability (NAL). A preliminary notice issued by the Commission or by the Enforcement Bureau or Media Bureau under delegated authority, notifying the recipient of a proposed forfeiture penalty, the reason for the proposed forfeiture, and an opportunity to provide a written response to the proposed forfeiture.

- j. Termination of Collection Action. Termination of Collection Action occurs when the Commission determines it has taken all appropriate efforts and (1) is unable to collect any substantial amount through its own efforts or through the efforts of others; (2) the Commission is unable to locate the debtor; (3) the costs of collection are anticipated to exceed the amount recoverable; (4) the debt is legally without merit or enforcement of the debt is barred by any applicable statute of limitations; (5) the debt cannot be substantiated; or (6) the debt against the debtor has been discharged in bankruptcy.
 - k. Trial *de novo*. Trial *de novo* in law literally means trial “from the beginning.” Pursuant to Sections 503(b) and 504(a) of the Communications Act, FOs that are not assessed by an administrative law judge are subject to a trial *de novo* when an enforcement action is brought by DOJ in a United States District Court. The government bears the burden of proving the violation and the liability for forfeiture.
5. BACKGROUND: The Commission, as well as the Commission’s Enforcement Bureau and Media Bureau acting under delegated authority, may issue a NAL proposing a forfeiture (also referred to as a CMP) against any person or entity that appears to have violated the Communications Act, a Commission rule, a Commission order, or a term or condition of a Commission authorization. In certain instances, a Citation, notifying a party of a violation of the Communications Act, Commission rule, or a Commission order and providing the party an opportunity to respond, must be issued prior to the issuance of an NAL. As set forth in Title 47, Chapter 1 of the Code of Federal Regulations (C.F.R.), the person or entity receiving an NAL will receive notification of the reason for the NAL, and be allowed a period of time (usually 30 days) to pay the proposed forfeiture amount or show in writing why the proposed forfeiture penalty should not be imposed or should be reduced. If the proposed forfeiture penalty is not paid in full in response to the NAL, the Commission or relevant B/O may cancel the proposed forfeiture, or issue an FO requiring payment of either the full or a reduced amount by a specific date. If the forfeiture is not paid, the case may be referred to OGC for possible referral to DOJ for action to enforce the forfeiture, provided that the case meets certain requirements, such as minimum monetary threshold. If DOJ accepts the case, it will file a complaint in a United States District Court seeking an order from the Court to enforce the forfeiture. The forfeiture amount is not a legally enforceable debt owed to the United States until either a partial payment of the forfeiture amount is made, or a court of competent jurisdiction has ordered payment and such order is final. In the alternative, the Commission, the relevant B/O acting under delegated authority, and the party may enter into a Consent Decree (“CD”) resulting in a voluntary contribution to the Treasury and compliance with certain other conditions. All CMPs that become legally enforceable debts owed to the United States are reported as such for financial accounting purposes.

Forfeiture payments are made through the Commission’s online fee filing system (Fee Filer), and the lockbox bank for deposit into the miscellaneous receipts fund of the Treasury.

6. POLICY:

The following FCC policy applies:

- a. Timing of Enforcement Actions: Assessment and enforcement of monetary forfeitures imposed by the Commission will be governed by procedures prescribed in 47 U.S.C. §§ 503, 504 and 47 C.F.R. § 1.80.
- b. Timing of Collection Actions. The Commission will determine if delinquent debt procedures are appropriate, after the conclusion of forfeiture enforcement proceedings. The Commission may determine that delinquent debt collection procedures are appropriate, but OMD-FO Demand Letters or other collection actions will not be issued or commenced until:
 - (1) The violator makes a partial payment towards the forfeiture amount set forth in the NAL or FO, and 30-days have passed since issuance of the NAL or FO pursuant to which the partial payment was made;
 - (2) The Commission receives from a court of competent jurisdiction a final order for payment; or
 - (3) The B/O confirms that the violator has failed to comply with the voluntary contribution and administrative compliance of the CD.
- c. Delinquent Debt. Legally enforceable delinquent debt will be transferred by OMD-FO to the Treasury in accordance with the Debt Collection Improvement Act of 1996 - i.e., 31 U.S.C. § 3711, Subpart O of the Commission's rules, and 31 C.F.R. § 285.12. Upon transfer to Treasury, the Commission will cease all collection activity related to the debt. The debt will be retained on the Commission's books.
- d. Installment Payments and Partial Payments. Under Commission rules, the Commission may allow a violator to pay the forfeiture amount under the terms of an installment payment plan administered by OMD-FO.

Partial payments will be accepted and applied in accordance with the Commission's rules. Upon receipt of a partial payment, and in the absence of an agreed-upon installment plan, OMD-FO will notify the violator through a Demand Letter that the remaining balance of the forfeiture penalty is a legally enforceable debt that is delinquent and the Commission will enforce debt collection procedures including assessment of interest and penalties, application of the Commission's Red Light Rule, and referral of the delinquent debt to Treasury.
- e. Collection of Interest, Penalties, and Assessments. Interest and penalties will be assessed as set forth in 31 U.S.C. § 3717 and 47 C.F.R. § 1.1940.
- f. Write-Off Debt and Suspension and Termination of Collection Activity. The Commission, through OMD-FO, will follow procedures in 31 C.F.R. §903.1 – 903.3, 47 C.F.R. § 1.1916, and OMB Cir. A-129 to Write-Off uncollectable debt and to suspend or terminate collection activity. Subsequently, the Commission may Close-Out the debt and issue the debtor a form 1099-C.

- g. Effect of Bankruptcy Proceedings on Collection Activity. Upon notification of bankruptcy, the Commission shall terminate collection activity on an enforceable debt and notify the Commission's OGC bankruptcy counsel to prepare a proof of claim. The Commission may continue collection activity subject to the provision of the Bankruptcy Code, or Bankruptcy Court Order, for any payments provided under a plan of reorganization.

7. RESPONSIBILITIES:

a. The Office of the Managing Director, Chief Financial Officer, shall:

- (1) Initiate collection of all civil monetary penalties that are legally enforceable debts;
- (2) Record into the Commission's financial system as accounts receivable all valid and legally enforceable debts arising from NALs, FOs and CDs;
- (3) Track proposed assessments and payment activities on each CMP imposed by the Commission or a B/O, whether or not the CMP is a legally enforceable debt;
- (4) Update the status of NALs, FOs, and CDs upon receipt or issuance of subsequent correspondence;
- (5) Administer the activities of the lockbox bank to provide a depository for payment of a civil monetary penalty;
- (6) Process documents/remittances received at the lockbox bank and forwarded to the Commission;
- (7) Notify the FCC OGC Litigation Division ("OGC/Litigation") if a partial or full payment is received for a case that has previously been forwarded to DOJ for enforcement;
- (8) Maintain financial files of legally enforceable debts, to include as applicable the NAL, FO, CD, court order, Claim Collection Litigation Report and related correspondence;
- (9) Refer all legally enforceable debts that are 120-days past due to the Treasury;
- (10) Obtain supporting documentation for all Intra-Governmental Payment and Collection ("IPAC") transactions received from DOJ or Treasury, and post IPAC payment receipt(s) transactions to the proper account(s);
- (11) Close out cases where the Outstanding Balance Due represents the amount retained by DOJ for the Civil Debt Litigation Collection Fee of 3%;
- (12) Maintain records to provide the Commission with reports on collection efforts and compliance with these procedures;
- (13) Ensure compliance with the Debt Collection Improvement Act of 1996;

- (14) Write-Off and Close-Out debt, and suspend or terminate collection activities, as appropriate;
- (15) Periodically review information recorded in the Commission's financial system for recording accounts receivable;
- (16) Review the violator's ability to pay in full the amount of the forfeiture assessment, and approve or disapprove requests for CMP installment payment plans;
- (17) Manage and maintain the CMP installment portfolio;
- (18) Update the Commission's financial system for recording accounts receivable on the status of the debtor's installment payment plan or default;
- (19) Forward financial documentation to OGC/Litigation upon request;
- (20) Obtain FCC OGC legal advice on procedures to follow pertaining to notices of bankruptcy, matters involving claims, administrative procedures, and/or litigation;
- (21) Make all financial records available to authorized Commission staff;
- (22) Notify B/Os that payment of a forfeiture has not been received by the required date;
- (23) Provide monthly reports to applicable staff in OMD-FO, Enforcement Bureau, Media Bureau and OGC/Litigation of CMPs with Outstanding Balance Due, and CMP payment receipt activity; and
- (24) Provide annual report to applicable staff in OMD-FO, Enforcement Bureau, Media Bureau and OGC/Litigation of CMPs aging data.

b. The Enforcement Bureau and Media Bureau shall:

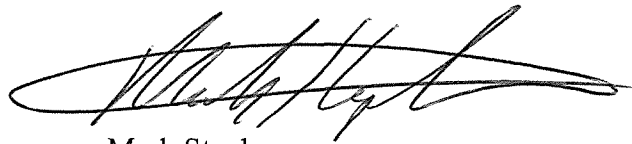
- (1) Initiate and issue NALs and FOs, in accordance with pertinent delegated authority provisions, and review and respond to requests for reconsideration or mitigation, where appropriate;
- (2) Negotiate and enter into CDs, where appropriate;
- (3) Provide notice of any NAL, FO, or CD and subsequent actions to OMD-FO;
- (4) Maintain supporting documentation (can be maintained electronically or in hard copy) pertaining to each forfeiture proceeding initiated until the proceeding is completed;

- (5) Forward the forfeiture case file to OGC/Litigation for review and timely referral to DOJ to ensure that a complaint may be filed before the expiration of the controlling statute of limitations, upon notification by OMD-FO that payment of a forfeiture has not been received by the required date, provided that the forfeiture amount exceeds the statutory minimum necessary for institution of collection proceedings;
- (6) Notify OMD-FO and close out the forfeiture case file upon notification that payment of the assessed forfeiture amount has been received in full, or that the enforcement or collection proceeding has been concluded;
- (7) Review all case files for further action upon notification by OMD-FO that payment is delinquent, and annually to determine whether the forfeiture proceeding should be terminated; and
- (8) Forward to OMD-FO any request for installment payment plan, and B/O installment agreements.

c. The FCC OGC/Litigation Division shall:

- (1) Receive forfeiture case files referred from the Enforcement Bureau or Media Bureau, and notify the relevant B/O or OMD-FO of additional documents or information needed;
- (2) Review referred forfeiture case file to determine whether to: return the case to the relevant B/O (e.g. because additional documentation is needed, or an administrative appeal is pending before the Commission, etc.), issue a Final Notice Letter to the subject of the forfeiture, refer the case to DOJ, or close the case and return it to the relevant B/O for termination of collection activity (e.g. because the forfeiture amount does not meet monetary thresholds established by DOJ regulations or individual United States Attorney's Offices; the statute of limitations in 28 U.S.C. § 2462 may bar the case or not permit sufficient time for DOJ to file an enforcement action; the subject is judgment proof; the amount is too insignificant to justify proceeding with a trial *de novo*; the claim cannot be substantiated by evidence);
- (3) Prepare a case file for the referred forfeiture and record case information in OGC tracking documents;
- (4) Time permitting, issue Final Notice Letter to the subject of the referred FO that the Commission has ordered payment of a forfeiture, and, where applicable, that the forfeiture may be referred to DOJ for enforcement if payment is not received;
- (5) Verify that subject of FO did not respond to Final Notice letter;
- (6) Prepare Claim Collection Litigation Report;

- (7) Refer forfeiture cases that meet the requirements set forth in 31 C.F.R. § 904 and all applicable documents to DOJ for enforcement and provide assistance to DOJ in the enforcement action;
- (8) Notify OMD-FO and the B/Os of cases declined by DOJ;
- (9) Notify the Assistant United States Attorney Office (AUSA) of any payments or other matters affecting the enforcement action;
- (10) Notify OMD-FO and relevant B/Os of the case status and disposition (e.g. partial payment, suit filed, DOJ declined, settlement, judgment, appeals, bankruptcy action, case closure by OGC) and provide copies of documents;
- (11) Notify OMD-FO and the relevant B/Os if DOJ has determined that an enforceable forfeiture is uncollectible, so that OMD-FO and the relevant B/O terminate and suspend collection activity; and
- (12) Furnish legal advice to OMD-FO and B/Os on matters involving claims, bankruptcy, administrative procedures, and/or litigation.

A handwritten signature in black ink, appearing to read 'Mark Stephens', with a large, sweeping horizontal stroke underneath.

Mark Stephens
Acting Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Regulatory Flexibility Act of 1980, as amended (P.L. 96-354) and the Small Business Regulatory Enforcement Fairness Act of 1996 (P.L.104-121).	
	Directive Number: FCCINST. 1158.2	Effective Date: September 15, 2011

- I. **PURPOSE:** To establish standard practices for implementation of the Regulatory Flexibility Act (“RFA”) and the Small Business Regulatory Enforcement Fairness Act (“SBREFA”) within the Commission.
- II. **CANCELLATION:** FCCINST 1158.1, "Regulatory Flexibility Act of 1980 (P.L. 96-354)," dated September 2006, is superseded by this directive.
- III. **BACKGROUND:** The RFA, as amended by SBREFA, is designed to focus agency consideration of the impact of proposed and final rules on small business, small non-profit organizations, and small government jurisdictions (collectively "small entities"). The RFA is a procedural statute that is designed to increase agency awareness and understanding of the impact of regulations on small business, to require agencies to communicate and explain their regulations to small entities, and to encourage agencies to provide flexibility and regulatory relief to small entities where appropriate. The RFA also has other requirements, including the publication of compliance guides, preparation of the semi-annual Unified Agenda, and an annual review of rules that are 10 years old and have a significant impact on a substantial number of small entities.
- IV. **SCOPE AND APPLICABILITY:** The procedures established herein apply to all proposed and final notice-and-comment rules that could have a "significant economic impact on a substantial number of small entities," and existing rules that have such an effect.
- V. **CROSS-REFERENCES:** Additional guidance is provided in internal documents specific to the projects; *e.g.*, the document entitled “Memorandum on Regulatory Flexibility” (“RFA Memorandum”) which is part of the Agenda Handbook and also can be found on the Office of Communications Business Opportunities’ (OCBO’s) website, <http://intranet.fcc.gov/ocbo/RegFlex.html> and the Small Entity Compliance Guide at <http://intranet.fcc.gov/ocbo/ComplianceGuides.html>.
- VI. **RESPONSIBILITIES:**
 - A. **Bureau and Office Chiefs.**
 1. Consistent with Commission internal guidelines, the following summarizes duties with regard to the preparation of each Certification, Notice of Proposed Rule Making (“NPRM”) and Report and Order (“Order”), respectively:

- a. for all rulemakings, consult with OCBO during the drafting stage about issues which may affect small entities; and
 - b. for NPRMs, determine whether the proposed rule(s) might have "a significant economic impact on a substantial number of small entities." *See* 47 U.S.C. §§ 601, 603-605. Although the RFA and the courts have not defined the terms "significant" or "substantial," the RFA Memorandum, at section IV, describes some considerations that can assist in assessing whether these thresholds have been met. These considerations include whether the proposed rules have a direct economic impact on small entities that cannot be described as *de minimis*. Proposed rules may have a direct economic impact by adversely affecting revenues or profit margins or by imposing undue administrative burdens. Agencies have broad discretion to determine the factors that should be considered in assessing the small business impacts of their regulations.
2. For certifications, if the proposed or final rule(s) appear to have a *de minimis* direct economic impact on small entities:
 - a. consult with OCBO;
 - b. complete an initial certification, as described in the RFA Memorandum, and include it in the NPRM and the Federal Register summary; and
 - c. complete a final certification, as described in the RFA Memorandum, to accompany the final rule(s) and to be included in the *Federal Register* summary.
 3. For all rulemakings where the proposed or final rule(s) could have a direct economic impact on small entities that cannot be described as *de minimis*:
 - a. consult with OCBO concerning any potential small entity issues;
 - b. For NPRMs, complete an initial regulatory flexibility analysis (IRFA) as described in the RFA Memorandum, and include it in the NPRM and the *Federal Register* summary;
 - c. For Orders, complete a final regulatory flexibility analysis (FRFA) as described in the RFA Memorandum, and include the agency's response, in detail, to any comments filed by the Chief Counsel for Advocacy of the SBA to the proposed rule(s) and a detailed statement of any change made to the proposed rule in the final rule as a result of the comments, *See* 5 U.S.C. Sec. 604(a)(3), *see also*, Secs. 604(a)(1) and 604(a)(2); also,
 - (i) publish the FRFA with the final rule(s) in the Order and in the *Federal Register* summary; and
 - (ii) complete a Compliance Guide for release following the publication of the final rule(s) in the *Federal Register*. Prior to release of the Compliance Guide, submit a draft to OCBO for review and coordination with the Enforcement Bureau and the Office of General Counsel. Compliance guides will be published on the FCC website, distributed to interested parties, and included in the agency's annual Report to Congress. The internal guidance manual concerning Compliance Guides can be found at <http://intranet.fcc.gov/ocbo/ComplianceGuides.html>. (SBREFA, sections 211, 212, 215; *see* 5 U.S.C. § 601 note.)

4. Submit semi-annually to OCBO a description of all current notice-and-comment rulemaking proceedings of the relevant Bureau or Office. *See* 5 U.S.C. § 602. All federal agencies are required to submit information, in a uniform format, to the General Services Administration (GSA) about regulations that are being considered or reviewed. GSA publishes a compilation of those submissions in a document entitled the “Unified Agenda of Federal Regulatory and Deregulatory Actions,” or “Unified Agenda.”
5. Submit annually to OCBO a list of the existing rules that have a significant economic impact on a substantial number of small entities, which are to be reviewed pursuant to Section 610 of the RFA during the succeeding 12 months. The rules to be reviewed are those promulgated 10 years prior to the year of the review. After publication of the list of rules, the Bureaus and Offices have the succeeding 12 months to review the rules utilizing the following factors:
 - a. the continued need for the rule;
 - b. the nature of complaints or comments received concerning the rule from the public;
 - c. the complexity of the rule;
 - d. the extent to which the rule overlaps, duplicates or conflicts with other Federal rules, and, to the extent feasible, with State and local governmental rules; and
 - e. the length of time since the rule has been evaluated or the degree to which technology, economic conditions, or other factors have changed in the area affected by the rule (5 U.S.C. § 610 (b)).

B. Office of Communications Business Opportunities.

1. Serve as the principal small business advisor to the Commission, Bureaus and Offices as provided in the Commission’s rules;
2. Develop, with the participation of Bureaus and Offices, policies, plans and programs to further the competitive concerns of small entities;
3. Manage the implementation of the RFA and SBREFA;
4. Advise Bureaus and Offices with regard to whether the proposed and final rules may have a significant impact on a substantial number of small entities;
5. Act as the Commission's liaison with the SBA;
6. Review NPRMs, Orders, and other items for Commission action to ensure consistency and compliance with the requirements of the RFA and SBREFA;
7. Solicit information, on a semi-annual basis, about current rulemaking proceedings for inclusion in the Unified Agenda;
8. Coordinate the submission of the description of the Commission’s current rulemaking proceedings to the GSA;
9. Review and coordinate the publication of Compliance Guides and distribute those guides to interested parties;
10. Prepare the agency’s annual Small Entity Compliance Guide Report to Congress;

11. Ensure that small entities obtain an opportunity to participate in any applicable rulemakings;
12. Solicit information, on an annual basis, about rules that are subject to review pursuant to Section 610 of the RFA. OCBO should solicit information no later than December 31st each year.
13. Coordinate the *Federal Register* publication, by March 31st of each year, of the list of existing ten-year-old rules subject to review for continuation, modification, or elimination;
14. Maintain an electronic tracking system to monitor the resolution, by the Bureaus and Offices, of public comments filed in response to the publication of the Section 610 list of rules;
15. Provide training, advice, and guidance on matters relating to the RFA and SBREFA by offering annual training seminars and quarterly Regulatory Flexibility clinics and by inviting SBA to hold regular sessions for Commission rule writers; and
16. Update this Directive to reflect changes in law or policy, as appropriate.

C. **Consumer and Governmental Affairs Bureau.**

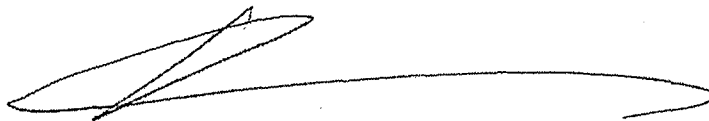
After Commission adoption of a notice-and-comment rulemaking proposal or order, transmit a copy of the item with certification of non-applicability of the RFA or with the regulatory flexibility analysis, as appropriate, to the Chief Counsel for Advocacy, SBA.

D. **Office of General Counsel.**

Provide legal advice concerning administrative law and litigation to OCBO and the other Bureaus and Offices on issues relating to the Administrative Procedure Act, RFA and SBREFA.

E. **Office of Managing Director**

Monitor Commission operations to ensure continued compliance with the policies and procedures specified in this Directive.

A handwritten signature in black ink, appearing to read 'David Robbins', with a long horizontal flourish extending to the right.

David Robbins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Freedom of Information Act (FOIA) Requests	
	Directive Number FCCINST 1179.2	Effective Date April 16, 2012

1. **PURPOSE:** To implement standard internal procedures for use within the Federal Communications Commission (FCC or Commission) in receiving, processing, and reporting on Freedom of Information Act (FOIA) requests. This directive supplements procedures in the FCC Rules and Regulations 47 C.F.R. §§ 0.460 and 0.461 and does not in any way alter the rights of the public to file FOIA requests.
2. **CANCELLATION:** This instruction supersedes FCCINST 1179.1 dated December 2006.
3. **BACKGROUND:** The FOIA, 5 U.S.C. § 552, as amended, makes many federal records available for public inspection. It ensures public access to Federal records in a reasonable, timely fashion.

The FOIA was most recently amended in 2007 by the Openness Promotes Effectiveness in our National Government Act, known as the OPEN Government Act. It made several procedural amendments to the FOIA, including revising the definition of news media requesters; specifying the manner of computing and tolling the time limits for responding to requests; requiring tracking of FOIA requests by agencies; amending the annual agency reporting requirements; amending the way agency records maintained by government contractors are treated under the FOIA; codifying the Chief FOIA Officer and FOIA public liaison position; setting forth new marking requirements for redactions of documents; and creating a new Office of Government Information Services (OGIS) as part of the National Archives and Records Administration (NARA).

4. **RESPONSIBILITIES:**
 - A. The Chairman of the FCC delegated responsibility to the Office of General Counsel (OGC) to serve as the Chief FOIA Officer for the Commission. As Chief FOIA Officer, the General Counsel is responsible for overseeing and monitoring the efficiency and effectiveness of the FOIA program.
 - B. The Office of Managing Director (OMD), Performance Evaluation and Records Management (PERM) is responsible for the administration and day-to-day management of the FOIA program. PERM serves as the FOIA Public Liaison and the FOIA Requester Service Center.

C. General Counsel:

- (1) Subject to the authority of the Chairman, the General Counsel serves as the Chief FOIA Officer for the Commission and is responsible for the Commission's efficient and appropriate compliance with the FOIA.
- (2) Monitors FOIA implementation throughout the Commission.
- (3) Reviews and reports, through the Chairman, on the Commission's performance implementing FOIA.
- (4) Prepares the annual Chief FOIA Officer Report.
- (5) Facilitates public understanding of the purpose of the FOIA with respect to the FCC.
- (6) Issues FOIA-related policy documents.
- (7) Serves as the FOIA coordinator for the Chairman and Commissioners.
- (8) Provides consultation on FOIA issues to B/Os and PERM when requested.
- (9) Consults with PERM when requested with respect to the category of the requester for fee assessment purposes. If there is a disagreement, OGC will make the final determination on the category of the requester.
- (10) Acts on requests for waiver of search, copying or review fees.
- (11) Prepares recommendations to the Commission on the disposition of applications for review (FOIA appeals) and represents the Commission in court actions involving FOIA matters.

D. Office of Managing Director/Performance Evaluation and Records Management:

- (1) Manages the FCC's FOIA program and the FOIA Requester Service Center.
- (2) Serves as the central control and contact point on all requests for records received pursuant to the FOIA, acknowledging receipt of all incoming FOIAs, processing and distributing initial FOIA requests to appropriate B/O for response, monitoring the B/O's progress in responding to requests, preparing and submitting all routine reports on the disposition of requests, and notifying Financial Operations (FO) of the amount to be billed to the requester.
- (3) Where multiple B/Os are likely to have responsive records, assigns lead B/O to prepare the initial response with the assistance of other B/Os.

- (4) Serves as the FOIA Public Liaison. Responds to public inquiries concerning the status of FOIA requests and addresses concerns about the processing of requests. Resolves disputes between the public and the Bureau/Office processing the request to the extent possible.
- (5) Leads efforts to consult with or refer a FOIA request to other government agencies and Departments when necessary, as described in section 6, *infra*.
- (6) Ensures customer-friendly responses to FOIA requests and FOIA related inquiries.
- (7) Reviews monthly report of delinquent accounts to ensure that requesters who have an outstanding financial obligation to the Commission do not obtain FOIA services until the debt is satisfied.
- (8) In consultation with the OGC, prepares the required annual report for submittal to the Department of Justice.
- (9) Maintains B/O records of FOIA requests, actions, and responses and disposes of these records in accordance with the provisions of the General Records Schedule 14 which pertains to FOIA records.
- (10) Establishes and maintains a FOIA home page on the FCC Website to explain the scope of the FCC's FOIA program to provide requesters with the option of submitting FOIA requests electronically. At a minimum, the FCC FOIA home page shall contain general information about the FOIA program, maintain an electronic reading room containing frequently requested information, FCC Annual FOIA Reports, a listing of the principal FOIA contacts at the FCC including the FOIA Liaison, and a FOIA (EFOIA) request form.
- (11) Establishes and maintains a FOIA home page on the FCC Intranet to expand the availability of FOIA documents to FCC staff. At a minimum the FCC FOIA Intranet page shall contain FCC B/O contact names and information, weekly FOIA reports, copies of incoming FOIA requests, fee waiver letters, Applications for Review (AFRs), decisions on AFRs, and copies of initial FOIA responses.
- (12) Manages the Privacy Act program. The Privacy Act of 1974, as amended (5 U.S.C. § 552a) is a companion to the FOIA. The Privacy Act and the FOIA have different procedures and exemptions. Employees who are involved with processing public requests should become familiar with procedures under both Acts. For additional information on the FCC's Privacy Act program, see 47 C.F.R. §§ 0.551-0.561 and FCCINST Directive 1113 (the Privacy Act Manual). For a listing of the Commission's systems of records, see <http://intranet.fcc.gov/omd/perm/privacyact/pra-systemrecord.html>.

- (13) Pursuant to the 2007 OPEN Government Act, designates a FOIA Public Liaison, "who shall assist in the resolution of any disputes": assign tracking numbers to FOIA requests that take longer than 10 days; provide systems determining the status of a request; and make the raw statistical data used in its reports available electronically upon request.

E. Bureau/Office Chiefs:

- (1) Designate an internal coordinator as point of contact to manage B/O FOIA actions. Encourage coordinators and others routinely involved with FOIA to attend FOIA training at least once a year from a recognized source of FOIA expertise (preferably the Department of Justice FOIA training).
- (2) Review response to FOIA requests, exercise final approval authority, and sign all FOIA correspondence as the responsible official. This responsibility may be delegated as appropriate.

F. Bureau/Office FOIA Coordinators:

- (1) Manage requests within B/O to ensure response within 20 business days or within an extension as permitted by law. B/O will make every effort to act on the request within 20 business days. B/O may extend that time by an additional 10 business days under certain circumstances (see 47 C.F.R. § 0.461 and section 5, Procedures below) or by agreement with the FOIA requester.
- (2) Inform requesters of any necessary extensions.
- (3) Notify PERM when a new response date has been extended or negotiated. Forward a copy of the letter of extensions and requests for additional time to PERM.
- (4) Notify PERM when a request has been withdrawn.
- (5) Review and act on requests for expedited processing of FOIA requests in accordance with 47 C.F.R. § 0.461(h). Expedited processing shall be granted to a requester demonstrating a compelling need that is certified by the requester to be true and correct to the best of his/her knowledge and belief. Notice of the determination as to whether to grant expedited processing shall be provided to the requester within 10 calendar days. The B/O that grants a request for expedited processing is expected to process the request as soon as practicable.
- (6) Determine applicable fees and receive requester's agreement to pay fees prior to fulfilling the request. Document all determinations that lead to a decision to charge or not to charge a FOIA requester. This can be done either by including in the written response the assessed charges, if any. Notify requesters by letter that they will be receiving under separate cover a bill for payment and instructions for payment.

(7) Mail response to the requester. Forward an electronic copy of the FOIA response letter to PERM.

(8) Keeps records documenting all responses (including records released or redacted and released) and fee determinations in accordance with the provision of the General Records Schedule 14 which pertains to FOIA records.

G. Administrative Services Center (ASC):

Immediately delivers all mail identified as a FOIA request to PERM.

5. PROCEDURES:

A. General:

As codified in 5 U.S.C. § 552(a)(6)(A) and (B), the FOIA requires a determination of “whether to comply” with a FOIA request within 20 business days. This 20 day period begins when PERM date stamps and logs the FOIA request into the database. The FCC may take an extension of 10 or more business days in “unusual circumstances” by providing the requester a written notice. Use of the additional 10 business days may be claimed for the following reasons:

- (1) it is necessary to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;
- (2) it is necessary to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or
- (3) it is necessary to consult with another agency having a substantial interest in the determination of the request or among two or more components of the Commission.

If it is not possible to locate the records and make the determination within the extended period, as described in section 0.461(g) of the Commission’s rules, the requester will be provided an opportunity to limit the scope of the request so that it may be processed within the extended time period, or an opportunity to arrange an alternative time frame for processing the request or a modified request, and asked to consent to an extension or further extension. Agreement of extensions should be documented in writing. If the requester does not agree to an extension, pursuant to section 0.461(g)(2) of the Commission’s rules, the request will be denied on the grounds that the custodian has not been able to locate the records and/or to make the determination within the period for a ruling mandated by the FOIA. In that event, the custodian will continue to search for and/or assess the records and will advise the requester of further developments; but the requester may file an application for review by the Commission. When action is taken by the custodian of the records, written notice of the action will be given. Records

will be made available with the written notice of action or as soon thereafter as is feasible.

B. Receipt:

The ASC, or the receiving B/O, will deliver all letters identifiable as requests for the inspection of records or as FOIA requests to PERM. The request will be given a control number and date stamped by PERM in order to establish the Commission's date of a proper request.

PERM will ensure that the proper B/Os receive the FOIA request within eight working hours or less. The B/Os must establish sufficient safeguards to ensure compliance with the relevant response period.

C. Processing. Prior to forwarding a request to a B/O for response, PERM will:

- (1) Determine the classification of a FOIA request on the basis of the interpretative guidelines issued by the Office of Management and Budget (codified in FCC rules at § 0.466) and/or through additional information obtained from the FOIA requester.
- (2) Determine and note on the cover sheet the proper time code to be used for processing a FOIA request.
- (3) Send a copy of requests for a waiver of review, search or copying fees (pursuant to 47 C.F.R. § 0.466 or 0.470(e)) to OGC.
- (4) Scan non-electronic materials and mount the FOIA requests to the Commission's Intranet FOIA site on a daily basis.
- (5) PERM shall forward a copy of any FOIA from major news media outlets to the Chief of the Office of Media Relations.
- (6) Requests for expedited processing shall be forwarded to OGC.

D. Responding:

- (1) Upon receipt, the B/O FOIA coordinator will:
 - (a) Determine if the FOIA request has been directed to the appropriate office. If it is determined that the FOIA request has been misdirected, promptly return the request to PERM for appropriate handling rather than forwarding it to another B/O.
 - (b) If a request is not specific enough, either notify the requester in writing or by telephone requesting a more complete description of the material requested. Clarification obtained orally must be confirmed in writing (including by email exchange). During this period the request may be tolled. However, note that the OPEN Government Act limits when and how often agencies are allowed to toll the 20-day time period. Agencies are allowed to

toll under two circumstances: (1) one time to obtain information from the requester; and, (2) as many times as necessary to clarify fee-related issues with the requester. B/Os should make an effort to ask all non-fee related questions at one time, since they are not allowed to toll the clock for additional requests to the requesters. Note that in either circumstance, the Commission's receipt of the requesters' response ends the tolling period and the response clock resumes. Tolling decisions must be provided to the requester within 10 business days after a request is properly received by the custodian of records, and as noted only one such request may be made for non-fee related questions.

- (c) Thoroughly search files and records for material requested. The cut off date for the search of records is the date the FOIA request is received, unless the requester specifies a date. See 47 C.F.R. § 0.461(f)(6). However, if a requester specifies an earlier or later date, it should be accommodated unless there are compelling reasons not to do so.
- (d) When requested records have been removed to storage in a Federal Records Center (FRC) (including the Commission's off-site storage facility), use Form A-113, "Request for Recall of Records" to retrieve the records. Across the top print in block letters "FOIA Request" and notify the requester in the written response that the files have been requested and that she/he will be told when the records are retrieved from FRC.
- (e) When records have been accessioned as permanent records to the National Archives, the FOIA requester should be advised in writing to contact the National Archives and Records Administration (NARA) for access. If all of the responsive records fall under this category, the request can be closed after such notification.
- (f) Make a determination of whether the request for release is routinely available, *i.e.*, for material normally available for public inspection such as license files or other public files (47 C.F.R. §§ 0.453, 0.455). If the request is routine, notify requester in writing of three options for obtaining the requested material:
 - (i) material is available for inspection and may be reviewed in person at the Commission's offices in Washington, D.C. between 8:30 am and 5:30 pm;
 - (ii) copies can be obtained (at their expense) from the FCC's duplicating contractor; or
 - (iii) copies are available on the Commission's website.

- (g) If the records are not routinely available for public inspection, determine whether any of the FOIA exemptions in section 6 of this instruction (see also 47 C.F.R. § 0.457(d)) apply. When redactions are made to a record being released, B/Os must indicate the amount of materials being redacted and indicate at the site of the redaction the FOIA exemption relied upon.
- (h) If making an adverse determination, the B/O shall notify the requester of that determination and of his/her appeals rights. A requester has the right to administratively appeal any adverse determination, including for example: denials of records in full or in part; "no records" responses, denials of requests for fee waivers; fee estimates; and denials of request for expedited treatment.
- (i) If records requested were generated outside the FCC and submitted under a request for confidentiality (47 C.F.R. § 0.459) or are deemed confidential (47 C.F.R. § 0.457), the B/O FOIA coordinator shall send a letter informing the original source of the document request with a copy to the party that submitted the FOIA request. The letter may be transmitted via e-mail if a functioning e-mail address of the original source is known. The letter shall include a full copy of the FOIA request and the name and address of the requester. In addition, the letter shall inform the original source of the sought-after records of its right to respond to the FOIA request within ten calendar days, explaining why any portions of these records are confidential commercial information that should be withheld in whole or in part pursuant to FOIA Exemption 4. The letter shall also indicate that the party that filed the FOIA request may file a reply within ten (10) business days of receipt of the response. In instances where there are many submitters involved, the notice may be either provided individually or by public notice. When a request for confidential treatment is denied, the person who submitted the records will have ten business days to seek review. If no request for confidentiality was submitted, the Commission assumes no obligation to consider the need of non-disclosure but, in unusual instances, may determine on its own motion that materials should be withheld from public inspection.
- (j) If the records are the property of another agency, the request will be referred to that agency for a response and the requester will be so advised. If another Federal agency has an interest in the records located in response to a FOIA request, that agency will be consulted prior to issuing a response.
- (k) Estimate search and review fees in accordance with the criteria established by 47 C.F.R. §§ 0.467 and 0.470. Factors to consider include time required, the grade of persons conducting the search and review and time needed to prepare responsive records. No fees will be assessed if the fees would be equal to or less than

\$15.00. See 47 C.F.R. § 0.470(f) and section 6 below for more detailed information on fees. If the Commission estimates that charges are likely to exceed the greater of \$25 or the amount which the requester indicated he or she is prepared to pay, then it shall notify the requester of the estimated amount of fees and provide the requester with the opportunity to revise or clarify the request. Initial FOIA letters will include a paragraph setting forth the applicable fees or the reason there are no fees for processing the request (see section E(1)(g) below). Note that the Commission's failure to comply with the statutory time limits may limit the Commission's collection of all applicable fees. If the Commission fails to meet the statutory or agreed-upon deadline, it cannot assess search fees from commercial requesters, or duplication fees from educational, noncommercial scientific institution, or representatives of the news media requesters.

- (1) When sending an electronic distribution that includes personally identifiable information (PII), any PII shall be attached as an encrypted file, consistent with the FCC's "Cyber Security Policy" (July 2011).
- (2) Granting or denying a request is done by the B/O that is the custodian of the records at issue based upon the provisions of the FOIA, FCC regulations, and precedents established by the courts and the FCC. A B/O may in its discretion determine who within the B/O shall issue the letter disposing of a FOIA request.
- (3) The OGC will provide advice in any case when requested. However, the OGC must be advised when a FOIA request involves classified materials or materials that may potentially be candidates for derivative classification, or if the B/O Chief believes that the decision to grant or deny a request breaks new ground (establishes instances of a new or different precedent) or when the B/O Chief is uncertain of an issue's reasonable potential for reversal on appeal. In addition, the OGC and PERM must always be given prior notice of any proposed disclosure when it involves:
 - (a) Information gathered by monitoring radio communications and other materials covered by Section 705 of the Communications Act, 47 U.S.C § 705;
 - (b) Materials covered by a FOIA exemption; and
 - (c) Data possibly protected by the Privacy Act (see FCCINST 1113.1).

E. Reporting:

- (1) The response letter should be prepared after a determination has been made. The response letter may be transmitted via e-mail if a functioning

e-mail address is known, with responsive records attached electronically. Any such electronic distribution shall ensure that sensitive information, particularly privacy data, is attached as an encrypted file, consistent with the FCC's "Cyber Security Policy." The response letter should contain the following elements and be provided consistent with this guidance:

- (a) Include the FOIA control number; the nature of the request and the Commission's understanding of the request.
- (b) Describe any tolled period, time extension and the reason for it (e.g., needed to search records of multiple Bureaus), or whether the deadline has been missed.
- (c) Identify records that are being released or if no responsive records have been located.
- (d) State the cut-off date used.
- (e) Describe the records or portions that are being withheld, whether in whole or in part, and the authority for the withholding, citing applicable exemption(s) and providing a clear explanation of the reasons the exemption(s) was invoked. Consider whether any reasonably segregable portion of the record may be released and explain the basis for this determination. Then, examine records or portions of records being withheld to determine if any discretionary releases may be made. Agencies are encouraged to make discretionary releases if there is no foreseeable harm that would result from the release, even if an exemption would apply to a record. Discretionary releases are probably most applicable for records withheld under exemption 5, but should be considered in all instances where records are withheld. However, Bureaus and Offices should be sure to consult with the OGC before making any discretionary releases.
- (f) If records are being released but copies are not being provided, explain when and where records are available.
- (g) Provide explanation of the FOIA fees being assessed. If no fees are being assessed, indicate why.
- (h) Include procedures and time limits for appealing the denial to the OGC. Use the following or similar language: "If you believe this to be a denial of your request, you may file an application for review with the FCC's Office of General Counsel within 30 calendar days of the date of this letter. 47 C.F.R. §§ 0.461(j) and 1.115." If a request for confidential treatment is denied, cite 47 C.F.R. § 0.461(i) (10 days to seek review of denial of confidentiality request in context of an initial FOIA decision). If a decision grants in part and denies in part a FOIA request and a request for confidential treatment, the FOIA requester will get 30 calendar days to seek review, and the party whose request for

confidentiality was denied in whole or in part will get 10 business days to seek review.

- (i) Include address, name, and title of persons responsible for denial.
 - (j) When sending an electronic distribution that includes personally identifiable information (PII), any PII shall be attached as an encrypted file, consistent with the FCC's "Cyber Security Policy" (July 2011).
- (2) When the response is prepared and sent to the requester, forward a signed electronic copy of the final response letter to PERM.
 - (3) If the request involves materials filed with a request for confidential treatment, a copy of the letter disposing of the request will be sent to the party that originally provided the records. The letter may be transmitted via e-mail if a functioning e-mail address of the original source is known.
 - (4) If an initial FOIA decision determines that material submitted in confidence should be released to the requester, the disclosure may not occur unless the submitter agrees to disclosure or the time for an appeal by the submitting party (10 business days) has passed.

- 6 INTERAGENCY COORDINATION: In the course of processing records responsive to FOIA requests, it is not uncommon to locate records which either originated with another agency or which contain information that is of interest to another agency. The long-standing practice in such situations is to either *refer* the requested record to the originating agency or to *consult* with the other agency or component that has equity in the document to get its views on the sensitivity of the content of the document prior to making a disclosure determination. Typically, agencies *refer* records for direct handling to another agency when the records originated with that other agency. By contrast, when records originated with the Commission, but contain within them information of interest to another agency, the Commission should *consult* with that other agency prior to making a release determination.

A. Threshold Considerations:

- (1) While the typical practice should be to refer records when they originated with another agency, agencies may jointly agree that the records can be handled as a consultation.
- (2) Referrals may only be made to other Federal agencies that are subject to the FOIA. Thus, a referral should not be made to Congress, the courts, state governmental entities, private businesses, or individuals. However, as discussed below, the FCC may consult with such entities as necessary, but must then make a disclosure determination and respond itself concerning those documents.

- (3) When the B/O FOIA Coordinators find that they routinely locate the same or similar types of documents or information that originated with another agency, or finds that it routinely receives for consultation or referral the same type of record or information from another agency, B/O FOIA coordinators should look for ways to collaborate to see if they can adopt standard processing procedures with regard to the documents or information that might reduce the number of referrals or consultations that need to be made.

B. Procedures for Making a Referral:

When records are located which originated with another agency, the records should ordinarily be referred to the originating agency for processing and direct response to the requester. The following steps should be taken when making a referral of documents to another agency, subject to the exceptions described below regarding coordinating a response.

- (1) Identify records appropriate for referral to other agencies as soon as practicable during the course of processing a request.
- (2) Prior to making the referral, review the records and include the FCC's disclosure recommendations in the referral memorandum in order to facilitate the processing of the referral by the receiving agency.
- (3) Send the documents, with the accompanying memorandum containing the FCC's disclosure recommendations, to the originating agency or agencies as soon as practicable during the course of the processing.
- (4) Include in the referral package the FOIA request number assigned by the FCC. That original FOIA request number should always accompany any communication concerning the referred documents. Also include a copy of the FOIA request.
- (5) Provide the date the request giving rise to the referral was received by the FCC.
- (6) Advise the FOIA requester that a referral of records has been made, provide the name of the agency to which the referral was directed, and include that agency's FOIA contact information.
- (7) Maintain a copy of the records being referred and the cover memorandum accompanying the referral.

C. Procedures Upon Receipt of a Referral:

When the FCC receives a referral of documents from another agency, the following steps should be taken to ensure efficiency and accountability.

- (1) Assign the FCC's FOIA tracking number to the referral so that it can be readily tracked.

- (2) Send the FOIA requester an acknowledgment of receipt of the referral and identify the agency that made the referral, subject to the exceptions described below for coordinating a response.
- (3) Include in the acknowledgement both the FCC's FOIA tracking number and the original FOIA request tracking number assigned by the agency making the referral so that the requester can readily link the referred records to his or her original request.
- (4) Provide the FOIA requester with a telephone line or internet service that can be used to obtain information about the status of the referred records.
- (5) Track the referral just as you would an incoming request and include it in the FCC's Annual FOIA Report.
- (6) Always include the original request number from the referring agency as well as our own referral number in any correspondence with the requester regarding the referred documents.
- (7) The referring agency should receive a copy of the response to the requester.

D. Exceptions to Standard Procedures for Making Referrals Coordinating the Response:

- (1) When the FCC locates in its files law enforcement records originating with a law enforcement agency or classified records originating with an agency that is a member of the Intelligence Community, the FCC shall respond to the requester itself, after coordinating with the law enforcement or Intelligence Community agency that originated the records unless the other agency prefers to respond.
- (2) However, where the involvement of the originating agency is not publicly acknowledged, the standard referral procedures are not appropriate, and the Commission will coordinate with the agency which originated the documents and then make the response itself. This may be the case if, for example, the FCC locates within its files records originating with a law enforcement agency, and if the existence of that law enforcement interest in the third party was not publicly known, or if the Commission locates within its files material originating with an Intelligence Community agency, and the involvement of that agency in the matter is classified and not publicly acknowledged. In such instances, disclosure of that law enforcement interest could cause an unwarranted invasion of the personal privacy of the third party or potentially could cause national security harms, and therefore shall not be disclosed.

E. Procedures for Coordinating a Response:

To avoid inadvertently invading an individual's personal privacy or inadvertently revealing protected national security information, requests involving unacknowledged law enforcement or national security records that originated with another agency should be coordinated with the originating agency before itself making a response to the requester according to the following steps. For documents involving Intelligence Community agencies, because the Commission might be unaware of the sensitivity of the documents at issue, it is important that no referral be made without first coordinating with the Intelligence Community agency involved.

- (1) Upon identification of unacknowledged law enforcement or Intelligence Community records, contact the agency originating such records to inquire whether that agency's involvement in the matter can be publicly acknowledged without invading personal privacy or causing national security harms. Provide copies of the request and the requested records as necessary to facilitate this process.
- (2) If the agency that originated the records advises that there are no privacy or national security harms at risk by virtue of their involvement, then the standard referral procedures outlined above can be followed. In those cases, the other agency will respond directly to the requester according to the standard referral process.
- (3) Otherwise, the FCC should coordinate with the agency that originated the records to determine how the records should be handled under the FOIA.
- (4) During the time the agency originally in receipt of the request is coordinating, the FCC shall respond to status inquiries made by the requester.
- (5) The agency that originated the documents and whose views are being sought is responsible, upon request, for promptly providing updated status information to the agency originally in receipt of the request. That agency shall work proactively with the receiving agency to ensure that the processing of the request is conducted efficiently and that the requester is not disadvantaged as a result of the coordination process. Moreover, to preserve the privacy and law enforcement interests at stake, the originating agency should promptly provide its views on the records so that they can be readily incorporated into the receiving agency's response letter.
- (6) The release determination for the records that are the subject of the coordination should be conveyed to the requester by the FCC.

F. Consultations:

- (1) It is appropriate to consult with another agency or entity which holds an interest (sometimes referred to as “equities”) in the documents that are the subject of a FOIA request. This most commonly arises when the Commission locates records in response to a request that originated with the Commission, but which contain within them information of interest to another agency or another component. In those situations, the Commission should consult with that other agency, or equity holder, to obtain its views prior to disclosure of the records.
- (2) Consultations, rather than referrals, are also appropriate when the FCC locates records in its files that originated with an entity that is not itself subject to the FOIA. The FCC may consult with that outside entity as part of its process of making a disclosure determination.

G. Procedures for Making a Consultation:

When consulting with another agency to obtain its views on disclosure, the following steps should be taken.

- (1) Utilize the most time-efficient mechanism in conducting the consultation. For example, in certain situations a phone call or e-mail to the agency whose views are being sought may be all that is required.
- (2) For consultations requiring a more extensive review by the other agency, provide copies of the documents at issue, a copy of the request letter, and any other information that may assist the other agency in its analysis.
- (3) Conduct consultations simultaneously, rather than sequentially, whenever possible, to ensure greater efficiency. When doing so, advise the receiving agencies of the other agencies that are also reviewing the documents.
- (4) When providing updates to requesters on the status of their requests, include information concerning ongoing consultations. Ordinarily, with the same exceptions noted above in the section on coordinating responses, the identity of the entity which is being consulted can be provided to the requester.

H. Procedures Upon Receipt of a Consultation:

Whenever the FCC receives a consultation request from another agency, it should be mindful of the need to respond as promptly as practicable to the consultation to facilitate the other agency’s ability to finalize its response to the request. To ensure greater accountability for the handling of consultations, the Department of Justice created a requirement that agencies include data in their Annual FOIA Reports each year regarding any consultations that they receive. Agencies must report in Section XII of their Annual FOIA Reports the number of consultations received, the number processed, and the number of consultations remaining

pending at the end of the fiscal year, including the dates the ten oldest pending consults were received and the number of days those ten oldest consultations have been pending.

Upon receipt of a consultation, agencies should take the following steps.

- (1) Assign the consultation a tracking number to facilitate its handling and inclusion in the FCC Annual FOIA Report.
- (2) Promptly provide the FCC's views on the disclosability of the contents of the records to the agency seeking the consultation. Utilize the most time-efficient method in doing so.
- (3) Continuously assess the need and frequency of the consultations so that the FCC can identify ways to streamline or eliminate the need for certain consultations.

7. FEES: Federal agencies are obliged to safeguard the public fisc and should not provide search, review, and duplication services at reduced or no cost except under circumstances provided for by the FOIA.

A. Search and Review Fees

- (1) An hourly fee shall be charged for recovery of full, allowable direct costs of searching for and reviewing records requested under 47 C.F.R. § 0.460(e) or § 0.461, unless such fees are restricted, reduced, or waived pursuant to 47 C.F.R. § 0.470. No fees will be assessed if the fees would be equal to or less than \$15. See 47 C.F.R. § 0.470(f). Agencies are prohibited from assessing search fees (or duplication fees if the requester is an educational or noncommercial scientific institution or a representative of the news media) if the Commission fails to meet the 20 business day (or 30 business days if extended in unusual or exceptional circumstances) response time limit.
- (2) Search fees may be assessed for time spent searching, even if the Commission does not locate any records or if the records are determined to be exempt from disclosure.
- (3) The Commission shall charge only for the initial review. The Commission shall not charge for subsequent review at the appeal level for an exemption already applied. However, records or portions of records withheld in full under an exemption that is subsequently determined not to apply may be reviewed again to determine the applicability of other exemptions not previously considered. The costs of such subsequent review, under these circumstances, are properly assessable.
- (4) If the estimated fees are less than \$15.00, no fees will be assessed. 47 C.F.R. § 0.470(f).

- (5) If the estimated fees are likely to exceed the greater of \$25 or the amount which the requester indicated he/she is prepared to pay, whichever is greater, then the B/O shall notify the requester of the estimated amount of fees. Such notice shall offer the requester the opportunity to confer with Commission personnel with the objective of revising or clarifying the request. See 47 C.F.R. § 0.467(e).
- (6) When a request exceeds \$250 and the requester has no history of payment, then the B/O may require the requester to make an advance payment of the full amount before processing the request.
- (7) If estimated fees exceed \$250 and the requester has a history of prompt payment, then the B/O shall notify the requester by written response and obtain satisfactory assurance of full payment.
- (8) When a requester has previously failed to pay a fee charged in a timely fashion (i.e., within 30 days of the date of the billing), PERM shall require the requester to pay the full amount owed plus any applicable interest as provided in section 0.468 and make an advance payment of the full amount of the estimated fee before processing the new or pending request.
- (9) In the cases of subparagraphs (5)-(7) above, the administrative time limits prescribed will begin only after the Commission has obtained satisfactory assurance of full payment or received the fee payment. See 47 C.F.R. § 0.469.

B. Fees are assessed as follows:

- (1) Commercial use requesters: When the Commission receives a request for documents for commercial use, the B/O will assess charges that recover the full direct cost of searching for, reviewing, including excising or preparing for release, and duplicating the records sought.
- (2) Educational and non-commercial scientific institution requesters and requesters who are representatives of the news media: The Commission shall provide documents to requesters in these categories for the cost of reproduction only, pursuant to 47 C.F.R. § 0.465, excluding reproduction charges for the first 100 pages, provided however, that requesters who are representatives of the news media shall be entitled to a reduced assessment of charges only when the request is for the purpose of disseminating information.
- (3) All other requesters: The requester is entitled to the first 100 pages and the first two hours of search time free of charge. The requester cannot be billed for review time.

8. EXEMPTIONS:

- A. The FOIA provides specific areas in which records are exempt from mandatory disclosure. When the public interest is served by release of the records, release

may be justified despite the applicability of the exemption. However, the Commission may be prohibited from disclosing some types of records (e.g., classified documents). A large number of administrative law and court decisions are available for direction in this area. See, e.g., the Department of Justice Freedom of Information Act Guide & Privacy Act Overview (most recent edition), found at http://www.justice.gov/oip/foia_guide09.htm or in Westlaw under the FOIA-GUIDE library.

B. The exemptions and their citations are:

- (1) Classified documents concerning national defense and foreign policy – (A) “specifically authorized under criteria established by Executive Order to be kept secret in the interest of national defense or foreign policy” and (B) “are in fact properly classified pursuant to such Executive Order” (5 U.S.C. § 552(b)(1));
- (2) Internal personnel rules and practices – matters “related solely to the internal personnel rules” (5 U.S.C. § 552(b)(2));
- (3) Information exempt under other laws – information “specifically exempted from disclosure by statute [other than the Privacy Act, 5 U.S.C. § 552b], provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld” (5 U.S.C. § 552(b)(3));
- (4) Confidential business information – “trade secrets and commercial or financial information obtained from a person and privileged or confidential” (5 U.S.C. § 552(b)(4));
- (5) Internal communications – “inter-agency or intra-agency memorandums or letters which would not be available by law to party other than an agency in litigation with the agency” (5 U.S.C. § 552(b)(5));
- (6) Protection of privacy – “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy” (5 U.S.C. § 552(b)(6));
- (7) Investigatory files – “records or information compiled for law enforcement purposes, not only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency of authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by

¹ Although the Commission does not have original classification authority, it may be directed to derivatively classify records.

a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual” (5 U.S.C. § 552(b)(7));

9. EXCLUSIONS:

The Freedom of Information Reform Act of 1986 provided a new mechanism for protecting sensitive law enforcement records under certain circumstances. In particular, the statute created three record exclusions which authorized agencies, under specified circumstances, to treat records as not subject to the requirements of the FOIA. See 5 U.S.C. § 552(c)(1)-(3). These are rarely invoked and involve criminal law enforcement or foreign intelligence situations. You should consult OGC before attempting to invoke these exclusions and should notify PERM of the initiation of consultation with OGC in this matter.

10. APPLICATION FOR REVIEW

A. General. There are two types of application for review:

- (1) When B/O denies the initial request for information in whole or in part, the requester may appeal to the Commission for review of that decision.
- (2) When the B/O's initial decision grants access to records provided to the FCC on a privileged or confidential basis, the source of the original materials may file an application for review requesting that the record be withheld from disclosure.

B. Appeals by Requesters:

- (1) The letter denying a FOIA request will be signed by the denying official and will notify the requester of the right to appeal to the Commission. The requester should be notified that he/she has 30 calendar days from the date of the written ruling to file a written application for review which must be mailed or delivered to the OGC.
- (2) OGC will consult with the B/O that issued the initial FOIA decision and may request that the B/O issue a supplemental response. OGC may attempt to resolve appeals by requesters or third parties.
- (3) The Commission will attempt to act on the appeal within 20 business days after its filing or as soon thereafter as possible. Applications for review are submitted to the full Commission for a vote. Decisions on applications for review shall include the names of the Chairman and Commissioners. The appellant should be informed about the FOIA


mediation services offered by Office of Government Information Services (OGIS).

C. Appeals by Third Parties:

- (1) If the FOIA request pertains to materials for which confidentiality has been requested, or material listed in 47 C.F.R. § 0.457(d), the person submitting the information will be provided with a copy of the incoming FOIA request, 47 C.F.R. § 0.461(d)(3).
- (2) If the FCC grants the request for the inspection of such records, the source of the material is provided a copy of the decision and notified that no records will be released for 10 business days after the date of the written ruling to allow the third party to file for an appeal of the decision. The written request for review will be delivered or mailed to OGC detailing the basis for requesting the protection.
- (3) The Commission will attempt to resolve the appeal within 20 business days or as soon thereafter as is possible.

D. Courts and Outside Review:

- (1) A party may appeal the Commission's decision to withhold records to the appropriate United States District Court pursuant to the jurisdictional provisions of 5 U.S.C. § 552(a)(4)(B).
- (2) If the statutory deadline for acting upon an initial FOIA request or an appeal is not met by the Commission, the requesting party may immediately seek judicial relief. Therefore, all efforts should be made to meet the FOIA's statutory deadlines or obtain consent by the requester to an extension of time.
- (3) Decisions to disclose records may also be appealed under provisions of the Administrative Procedure Act or the Privacy Act.
- (4) FOIA requesters may also take advantage of mediation services offered by the Office of Government Information Services as a non-exclusive alternative to litigation.

A handwritten signature in black ink, consisting of a series of overlapping, sweeping strokes that form the name 'David B. Robbins'.

David B. Robbins
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	Title	
	Management of FCC Motor Vehicles	
	Directive Number FCCINST 1194.2	Effective Date September 19, 2012

1. **PURPOSE:** This directive sets forth the Federal Communications Commission's (Commission or FCC) policies, procedures, and responsibilities relating to requesting, operating, maintaining, managing, securing, and reporting of the Commission's owned or leased motor vehicles.
2. **CANCELLATION:** This instruction supersedes FCCINST 1194.1, dated November 2008.
3. **BACKGROUND:** Passenger carrier utilization of Government owned/leased vehicles is governed by 31 U.S.C. § 1344. Funds available to a Federal agency, by appropriation or otherwise, may be expended by an agency for the maintenance, operation, or repair of any passenger carrier only to the extent that such carrier is used to provide transportation for official purposes.
4. **SCOPE AND APPLICABILITY:** This directive applies to the use of Commission owned/leased vehicles by personnel assigned to the FCC. Utilization of Commission owned/leased vehicles by the Enforcement Bureau (EB) and Public Safety & Homeland Security Bureau are also governed by their respective Bureau Standard Operating Procedures. Utilization of FCC owned/leased vehicles by motor vehicle operators assigned to the Office of Managing Director, Associate Managing Director - Administrative Operations (AMD-AO), Administrative Services Center is also governed by Standard Operating Procedures, dated April 12, 2010.
5. **DEFINITIONS:** Definitions of the terms "incidental operator", "motor vehicle", and "operator" as used in this directive are found in 5 C.F.R. § 930.102 of the Office of Personnel Management regulations.
6. **POLICY:**
 - a. **Driver's Requirements.** All employees and contractors required and authorized to operate a motor vehicle in the performance of their duties must meet applicable state requirements and maintain a good driving record. Motor vehicle drivers are responsible for the safe operation of FCC owned/leased vehicles in accordance with traffic laws in the state(s) and local jurisdiction in which they operate. Drivers are required to have in their possession at all times when operating a Government owned/leased vehicle their valid operator's permit for the type of vehicle being operated. Annual safety training will be required to encourage safe driving.
 - b. **Official Use Requirement.** Commission owned or leased vehicles will only be used in the performance of official duties, or in emergencies threatening loss of life or property. As a general rule, whenever transportation is essential to the successful operation of the

FCC's mission, it will be considered as official use. Conflicts will be resolved in favor of strict compliance with the statutory restriction on using government transportation for unofficial purposes (*see* 31 U.S.C. § 1344, *see also* 41 C.F.R. § 102-34.220 (describing official use of motor vehicle owned or leased by the government)).

- c. Prohibition against Home-to-Work Transportation. With the limited exception provided below, home-to-work (portal-to-portal) transportation of FCC employees in normal duty (non-travel) status, performing duties at their place of employment, is not permitted, unless authorized in writing by the Chairman under the provisions of 31 U.S.C. § 1344 or 41 C.F.R. § 102-5. However, Enforcement Bureau field personnel shall act in accordance with instructions contained in EB's Vehicles Manual:
<http://eb.fcc.gov/VehiclesManual/VEHMAN.pdf>
- d. Use of Vehicles May be Authorized for Government-Approved Travel. An FCC employee in travel status may be authorized to use a government vehicle to ride from his/her home to the airport/train station or from the airport/train station to his/her home when traveling on official business. The home-to-work restrictions in section 5(c) above do not apply to employees on official travel (41 C.F.R. § 102-5.20). The FCC has a statutory duty to select the method of transportation that is most advantageous to the Government and the most expeditious means practicable commensurate with the nature and purpose of the duties of the employee requiring such travel, when cost and other factors are considered (5 U.S.C. § 5733; 41 C.F.R. § 301-70.101(a)).
- e. Restrictions on Who May Ride in Vehicles. Only persons traveling on official Commission business may ride in Commission vehicles. Their business must be specifically related to approved programs. Before allowing other persons to ride in a Commission vehicle, employees must consider the impact on the performance of official duties and the ability to justify their decision should there be a complaint or an accident.
- f. Penalties for Unauthorized Use. Any officer or employee who willfully uses or authorizes the use of such vehicle, for other than official purposes, shall be suspended for at least one (1) month or a longer period when warranted, or removed by the Chairman (31 U.S.C. § 1349).
- g. Prohibition against Personal Use. Commission owned or leased vehicles shall not be used for personal business under any circumstances. Employees shall exercise discretion to avoid any situation which may convey an impression that a Commission vehicle is being used for unofficial purposes.
- h. Safety Requirements. Anyone driving or riding in a vehicle on official business must wear a safety belt at all times when the vehicle is moving. Operators shall exercise all possible care to drive safely and defensively to avoid accidents. Operators shall determine that the vehicles are in proper operating condition before driving them, and shall notify the supervisor if the vehicles are inappropriate for use or in poor operating condition.
- i. Prohibition on Smoking. The Commission prohibits smoking in agency owned and leased motor vehicles.
- j. Hands-Free Units. Drivers are required to use the hands-free feature in the vehicle (If equipped) or an ear piece while driving in the District of Columbia and any State that

requires the use of hand-free units. Cellular phones will be used by the drivers for official business only. The use of the cellular phones by drivers for personal calls, incoming or outgoing, is prohibited.

7. VEHICLE MANAGEMENT:

- a. It is the Commission's policy to develop an efficient and economical Vehicle Management Program to ensure that adequate transportation is available to meet the FCC's mission requirements.
- b. As part of any efficient and economical Vehicle Management Program to be developed and maintained by the agency, priority for use of Commission owned or leased vehicles shall be given to FCC personnel in the following order:
 - (1) The Chairman;
 - (2) Commissioners;
 - (3) The Chairman's Chief of Staff;
 - (4) Bureau Chiefs and Office Directors;
 - (5) Deputy Bureau Chiefs and Deputy Office Directors (Federal agents requiring the use of an official government vehicle in the performance of their duties associated with an investigation shall be given the priority of a Deputy Bureau Chief and Deputy Office Director);
 - (6) All other Commission staff.

In accordance with this order of priority, a reservation for the use of a Commission owned or leased vehicle by agency personnel shall be cancelled if agency personnel with higher priority subsequently requests use of a motor vehicle for official use at the same time, and additional vehicles are not available. In such instances, Commission personnel shall be informed at the earliest practicable time that their reservation to use a Commission owned or leased motor vehicle has been cancelled.

- c. Headquarters vehicles will be dispatched from a central dispatch and control system to give the flexibility needed to meet changing mission requirements.
- d. FCC vehicles assigned to Headquarters will be garaged at the FCC in the spaces reserved for this purpose, in order to support operations.

8. HEADQUARTERS VEHICLE SERVICES:

- a. Generally, FCC vehicles may not be used as a first resort for transportation needs. Other modes of transportation, consistent with operational requirements, should be first considered by the availability of scheduled services as listed below:
 - (1) Scheduled public transportation - Metro transit cards are available for official travel;
 - (2) Taxicabs on a reimbursable basis; and,

- (3) Voluntary use of a privately owned motor vehicle on a reimbursable basis for out of town trips, such as to FCC facilities in Gettysburg, Pennsylvania and Columbia, Maryland.
- b. Vehicular services may be requested via e-mail using the electronically generated FCC Vehicle Request Form. The form may be found at:
<http://intranet.fcc.gov/omd/hrm/fccforms.html>. Requests must include:
 - (1) The date that the vehicle is required;
 - (2) The time that the vehicle is required;
 - (3) The number of passengers making the requested trip;
 - (4) An indication if the driver will be required to wait;

Note: As a general rule, drivers should not be requested to wait for passengers. However, drivers shall wait for the Chairman, Commissioners, the Chairman's Chief of Staff, and Bureau/Office Chiefs when they are making appearances on Capitol Hill or other such official events as appropriate.

 - (5) The destination of the trip clearly stated; and
 - (6) The requester's name and telephone number.
- c. With the exception of the Chairman, Commissioners, and the Chairman's Chief of Staff, all personnel must submit the FCC Vehicle Request Form in advance of their scheduled trip. To aid the process of scheduling the use of Commission vehicles, requests for vehicular service should be submitted as soon as the requirement is known.
- d. All trips originating from FCC headquarters will depart from the horseshoe driveway at the 12th Street side of the building.
- e. If a passenger is delayed by more than ten (10) minutes from the scheduled time of departure, the Administrative Services Center must be notified.
- f. With the exception of the Chairman, Commissioners, and the Chairman's Chief of Staff, at the conclusion of the trip, at least one passenger will be required to sign the FCC Vehicle Request Form in the block indicating that the trip was for official government business. For the Chairman, Commissioners, and Chairman's Chief of Staff, submitting the electronically-generated FCC Vehicle Request Form shall serve as a certification that the request is for official government business.

9. RESPONSIBILITIES:

- a. The Managing Director is responsible for the FCC's Vehicle Management Program and will ensure compliance with applicable Federal statutes and regulations.
- b. The Associate Managing Director - Administrative Operations is responsible for overseeing the FCC's Vehicle Management Program at FCC Headquarters and

Commission facilities in Gettysburg, Pennsylvania and Columbia, Maryland to ensure that vehicle utilization is only for official business.

c. The Manager, Administrative Services Center is responsible for:

- (1) Development and management of the FCC's Vehicle Management Program;
- (2) Maintaining and updating vehicle data, including required reports;
- (3) Establishing a maintenance program to ensure appropriate standards are achieved;
- (4) Ensuring against vehicle misuse, abuse, and unofficial use by FCC personnel;
- (5) Administering a safety program for all motor vehicles and operators;
- (6) Reporting motor vehicle accidents to the Office of General Counsel (OGC) and the Office of Managing Director (OMD), and maintaining records on vehicle accidents and safety issues;
- (7) Managing the accounts for rental of leased General Services Administration (GSA) pool vehicles for Headquarters, Gettysburg, Pennsylvania, and Columbia, Maryland; and
- (8) Maintaining and updating standard operating procedures which contain instructions and guidance to Headquarters, Gettysburg, Pennsylvania, and Columbia, Maryland personnel on the policies and procedures related to the use of Government owned/leased motor vehicles.

d. The Enforcement Bureau, Office of Management and Resources, is responsible for:

- (1) Developing and managing EB's Field Vehicle Management Program;
- (2) Developing and maintaining a comprehensive database of motor vehicle usage including compilation of data from Motor Vehicle Operation Reports (FCC Form A-344) and submission of the annual Report of Motor Vehicle Data to GSA on behalf of the Commission;
- (3) Compiling energy usage data (fuel consumption) and submitting the annual usage report to GSA for the agency;
- (4) Issuing license plates for FCC owned/leased vehicles and maintaining a record of such assignments for the agency;
- (5) Managing EB's accounts for rental of leased GSA pool vehicles;
- (6) Reporting motor vehicle accidents to the OGC and the OMD, and maintaining records on vehicle accidents and safety issues for EB;

- (7) Maintaining and updating Standard Operating Procedures which contain instructions and guidance to EB personnel on policies and procedures related to the use of Government owned motor vehicles; and
 - (8) Developing the EB's Vulnerability Assessment Report for Vehicle Use – Field, to ensure against fraud, waste and abuse.
- e. The Public Safety & Homeland Security Bureau, Operations and Emergency Management Division, is responsible for:
 - (1) Developing and managing PSHSB's Field Vehicle Management Program;
 - (2) Compiling energy usage data (fuel consumption) and submitting the annual usage report to EB to be compiled for the agency;
 - (3) Reporting motor vehicle accidents to the OGC, the OMD, and their vehicle leasing company and maintaining records on vehicle accidents and safety issues for PSHSB;
 - (4) Maintaining and updating Standard Operating Procedures which contain instructions and guidance to PSHSB personnel on policies and procedures related to the use of Government owned motor vehicles; and
- f. The Financial Operations Center, Accounts Processing Group is responsible for managing the agency's U.S. Government National Charge Card Program and issuing credit cards for use with FCC owned/leased vehicles.
- g. Each Bureau/Office is responsible for:
 - (1) Submitting Motor Vehicle Operation Reports (FCC Form A-344) to EB annually or when a vehicle is acquired, transferred or disposed of;
 - (2) Submitting annual vehicle fuel consumption reports (FCC Form A-344) of gasoline/diesel fuel consumption to EB;
 - (3) Maintaining a file on those employees who are qualified and authorized to operate Government owned/leased vehicles, including incidental drivers, in accordance with 5 C.F.R. §§ 930.109, 930.110;
 - (4) Reporting motor vehicle accidents to the OGC and the OMD, and maintaining records on vehicle accidents.
- h. Motor Vehicle Operators are responsible for:
 - (1) Providing the FCC Safety and Health Manager with their drivers license number upon request;
 - (2) Completing the OPM Physical Fitness Inquiry for Motor Vehicle Operators Form, OF-345 and a Federal Occupational Health (FOH) Authorization for Medical Release Form FOH-6 ME. The FOH form allows the FCC to release form OF-345 to the Federal Occupational Health Physician for review and allows the Federal

Occupational Health Physician to discuss relevant information with the FCC Safety and Health Manager as necessary.

- (3) Motor vehicle operator(s) assigned the responsibility for operating the Agency's owned/leased cargo truck with a gross combination weight (GCW) of 26,001 or more pounds, required to acquire and maintain a CDL and Medical Examiner's Certificate in accordance with the Commercial Motor Vehicle Safety Act, April 1, 1992.

10. PERIODIC DRIVER REQUIREMENTS REVIEW:

- a. In accordance with 5 CFR §§ 930.105 and 109, the FCC must review the authorization of the employees who operate a Government-owned or leased vehicles as part of their duties, at least once every 4 years to ensure that those employees meet the following requirements:
 - (1) Possess a safe driving record; and
 - (2) Possess a valid State driver's license.
- b. The FCC will meet this requirement by obtaining a copy of the employee's driving record through the Department of Motor Vehicles. This will be done at least every four years in conjunction with the required medical review.

11. PERIODIC MEDICAL REVIEW:

In accordance with 5 CFR § 930.109 the FCC must ensure at least once every 4 years, that those employees who operate Government-owned or leased vehicles as part of their duties, are medically able to do so without undue risk to themselves or others. This will be accomplished by:

- a. Requiring all employees who operate a government motor vehicle as part of their duties, to complete and submit Form OF-345 and FOH Form FOH-6 ME to the Safety and Health Manager upon request, but not more than four year intervals;
- b. The FCC Safety and Health Manager will submit the form OF-345 and FOH Form FOH-6 ME to a Federal Occupational Health Physician for review;
- c. The Federal Occupational Health Physician will reviews the form and provide a letter to the FCC Safety and Health Manager stating whether or not the employee is medically able to operate a government motor vehicle or leased vehicle;
- d. The FCC Safety and Health Manager will provide the Bureau/Office with a copy of the suitability letter (not the medical documentation); and
- e. The FCC Safety and Health Manager will direct the FCC Nurse to develop a medical record for each motor vehicle operator to house Form OF-345 and FOH Form FOH-6 ME and the original suitability letter from the Federal Occupational Health Physician.

Note: Forms OF-345 and FOH Form FOH-6 ME will be maintained in the FCC Health Center medical records file, which are maintained consistent with the FCC's Privacy Act

System of Records and with all applicable federal laws, rules and regulations regarding confidentiality of records including the Privacy Act (5 U.S.C. Section 552a). These records will not be released to unauthorized personnel without the prior written consent of the employee.

12. FINES/ACCIDENTS:

Employees of federal agencies who operate vehicles for official purposes should be aware that they are subject to all traffic laws and regulations promulgated by any level of government of any authorized public entity. Responses to citations, tickets, payment of fines, and any court appearances are the personal responsibilities of the vehicle operators. All citations, tickets, fines, court appearances and accidents must be immediately reported to the OGC and the OMD.


13. CORRECTIVE ACTIONS:

- a. Office of Personnel Management regulations at 5 C.F.R. § 930.113 require that an agency will take adverse, disciplinary, or other appropriate action against an operator or an incidental operator in accordance with applicable laws and regulations. Agency orders and directives will include the following reasons among those constituting sufficient cause for such action against an operator or an incidental operator:
 - (1) The employee is convicted of operating under the intoxicating influence of alcohol, narcotics, or pathogenic drugs.
 - (2) The employee is convicted of leaving the scene of an accident without making his or her identity known.
 - (3) The employee is not qualified to operate a government owned/leased vehicle safely because of a physical or pre-existing medical condition. In making such a determination, consult a Federal medical officer or other medical authority as appropriate.
 - (4) The employee's state driver's license is revoked.
 - (5) The employee's State license is suspended. (Note: The agency may continue the employee in his or her position for operation of Government-owned or -leased motor vehicles on other than public highways for not to exceed 45 days from the date of suspension of the State license).
- b. If a supervisor has reason to believe an employee has developed unsafe driving habits (multiple accidents, tickets, etc.), the supervisor will gather all information, facts, and circumstances leading to and supporting their concern and discuss them with the employees Bureau/Office Chief, and if appropriate, District Director. If higher-level concurs with the supervisor's concern, then the supervisor will promptly prepare a written report detailing the circumstances and contact Human Resource Management with a recommended course of action.

14. ETHICAL CONDUCT:

To ensure that every citizen can have complete confidence in the integrity of the Commission, each Commission employee shall adhere to the Commission's Code of

Conduct (Code of Conduct) set forth in the Policy for Detecting and Deterring Fraud and Promoting Ethical Conduct Within the Federal Communications Commission (Anti-Fraud Directive, FCCINST 1102.5, effective July 2011) with regard to operating or using Commission owned or leased motor vehicles. The Code of Conduct, which summarizes the Fourteen Principles of ethical conduct (Anti-Fraud Directive, section 4B(1)-(14)), is designed to deter wrongdoing and promote, among other things: (1) compliance with applicable governmental laws, rules, and regulations; and (2) the prompt internal reporting of violations of the Code of Conduct to an appropriate person or persons identified herein. All employees shall report instances of suspected fraud and illegal acts to their supervisor, manager or other appropriate Commission officials, including but not limited to, the Commission's Office of Inspector General or OGC in accordance with the Commission's Anti-Fraud Directive.



David Robbins
Managing Director

Federal Communications Commission Washington, D.C.	TITLE	
	Policies on Text Messaging While Driving	
	Directive Number: FCCINST 1195.1	Effective Date: May 31, 2010

FCC Directive

1. **PURPOSE.** This Directive implements the requirements of Executive Order 13513, “Federal Leadership on Reducing Text Messaging While Driving,” by establishing the Federal Communications Commission (FCC) policy on text messaging by employees when driving Government Owned Vehicles (GOVs), leased or rented vehicles, when driving privately owned vehicles (POVs) on official Government business, or when using electronic equipment supplied by the Government while driving. This Directive also implements the requirements of the Executive Order that directs the FCC to encourage federal contractors and subcontractors and recipients and subrecipients of grants and cooperative agreements to adopt and enforce policies that ban text messaging when driving company owned, leased or rented vehicles or GOVs, or when driving personally owned vehicles, leased or rented vehicles while on official Government business or when performing any work for or on behalf of the Government.

2. **REFERENCES.**
 - (a) Executive Order 13513, “Federal Leadership on Reducing Text Messaging While Driving,” October 1, 2009.
 - (b) 5 U.S.C. 7902(d) “Safety Programs.”

3. **SCOPE.** This Directive applies to all FCC employees and contractors:
 - (a) driving a GOV, or driving a POV while on official Government business; or
 - (b) using any electronic equipment supplied by the Government while operating any vehicle at any time.

Voluntary compliance with this Directive is encouraged even when a Federal employee is utilizing a personal electronic device and driving a POV while off-duty.

4. DEFINITIONS. For purpose of this Directive, the following definitions shall apply:

- (a) Motor vehicle: means any vehicle, self-propelled or drawn by mechanical power, designed and operated principally for use on a local, state or federal roadway, but does not include a military design motor vehicle or any other vehicle excluded under Federal Motor Vehicle Regulation 102-33.20.
- (b) Texting or text messaging: means reading from or entering data into any handheld or other electronic device (including, but not limited to, cell phones, navigational tools, laptop computers or other electronic devices), including for the purpose of Short Message Service (SMS) texting, e-mailing, instant messaging, obtaining navigational information or engaging in any other form of electronic data retrieval or electronic data communication. The term does not include the use of a cell phone or other electronic device for the limited purpose of entering a telephone number to make an outgoing call or answer an incoming call, unless this practice is prohibited by state or local law. The term also does not include glancing at or listening to a navigational device, a communications receiver, or a radio direction finder that is secured in a commercially designed holder affixed to the vehicle, provided that the destination and route, or adjustments to communications receivers and direction finders, are programmed into the device either before driving or while stopped in a location off the roadway where it is safe and legal to remain stationary.
- (c) Driving: means operating a motor vehicle on a roadway, including while temporarily stationary because of traffic congestion, a traffic signal, a stop sign, another traffic control device. It does not include being in your vehicle (with or without the motor running) in a location off the roadway where it is safe and legal to remain stationary.

5. BACKGROUND. Executive Order 13513, "Federal Leadership on Reducing Text Messaging While Driving," establishes a Federal Government-wide prohibition on the use of text messaging when driving a GOV, when driving a POV on official business or when using Government-supplied equipment while driving any vehicle. Implementation of the Executive Order will help save lives, reduce injuries, and set an example for state and local governments, private employers and individual drivers. Extending this policy to cover Federal contractors and grantees is designed to promote economy and efficiency in Federal procurement and grant implementation.

6. POLICY. It is the FCC policy to:

- (a) ban any and all text messaging by all FCC employees (i) when driving a GOV, (ii) when driving a POV while on official Government business; and (iii) using electronic equipment supplied by the Government when driving any vehicle (even during off-duty hours);

- (b) take appropriate disciplinary action for violation of this mandatory ban on texting, up to and including removal from Federal Service, as outlined in Section 9 of the Directive; and
- (c) encourage FCC employees; contractors; and their families to refrain from texting, or from engaging in any behavior that distracts attention from driving safely, at any time.

7. OBJECTIVES. The objectives of the mandatory ban on text messaging are to:

- (a) reduce injuries and fatalities resulting from traffic crashes involving employees;
- (b) encourage Federal contractors and subcontractors and recipients and subrecipients of grants and cooperative agreements to establish workplace safety policies to decrease crashes caused by distracted drivers; and
- (c) encourage agency employees and their families to voluntarily comply with the text messaging policy while off duty.

8. RESPONSIBILITIES.

- (a) The Office of Managing Director, Associate Managing Director, Administrative Operations shall, within 30 days of the effective date of this Directive, establish and disseminate FCC-wide contractual language to be included in future contracts encouraging contractors and subcontractors to comply with the policies contained in this Directive.
- (b) FCC officials shall:
 - (1) require all employees to comply with the text messaging ban imposed by this Directive and encourage them to refrain from text messaging while driving in other circumstances not covered by the Directive;
 - (2) direct the head of the procurement office to (i) comply with requirements developed to implement the Directive and encourage contractors and recipients and subrecipients of grants and cooperative agreements to adopt and enforce on-the-job policies banning text messaging for their employees when driving GOVs, or when driving POVs while on official Government business; and (ii) to comply with applicable federal procurement or grant regulations that may be adopted to ban texting messaging;
 - (3) participate in and support promotional programs and activities on the safety risks associated with distracted driving;
 - (4) issue a broadcast announcement to all employees and contractors reminding them of the provisions of this Directive at least annually;
 - (5) assign adequate personnel and resources to satisfy the requirements of this Directive;

- (6) beginning on January 31, 2011, file an annual report with the Managing Director identifying all violations of this Directive that occurred during the previous 12-month period and the disciplinary or corrective action imposed for each such violation;
 - (7) notify the U.S. Department of Transportation of measures undertaken to implement this Directive within 30 days of its effective date.
- (c) FCC Managers and Supervisors shall:
- (1) implement the requirements of this Directive;
 - (2) take prompt disciplinary or other appropriate action in accordance with agency policy and in consultation with the Human Resource Management office for violations of this Directive and report all violations to the Labor Relations and Performance Management Service Center;
 - (3) ensure that newly assigned personnel receive orientation information within 30 working days of employment with the FCC outlining the provisions of this Directive;
 - (4) periodically remind employees of this Directive and the ramifications and consequences of text messaging when driving a GOV, or when driving a POV while on official business or when using electronic equipment supplied by the Government while driving; and
 - (5) provide suggestions to the agency Safety and Health Manager, as appropriate, to promote and encourage employee and contractor compliance with this Directive.
- (d) FCC employees shall be familiar and comply with Federal, state, local and FCC motor vehicle safety requirements and policies, including the FCC's mandatory ban on text messaging as outlined in this Directive.
- (e) Chief, Contracts and Purchasing Center shall, upon receipt of applicable regulations, include contractual language as provided by the federal procurement and grant regulations in future contracts, grants and cooperative agreements that require contractor and grantee personnel to comply with the policies contained in this Directive. Until such regulations banning text messaging are adopted, the Contracts and Purchasing Center shall encourage contractors and grantees to adopt text messaging bans substantively comparable to Executive Order 13513.

9. DISCIPLINARY AND CORRECTIVE ACTION.

- (a) Failure to comply with this Directive may result in disciplinary action. Applicable consequences may include official reprimand, suspension from pay and duty, removal from Federal service, or other actions in accordance with law and agency policy.

- (b) Failure to comply with this directive may result in immediate suspension of authority to drive a GOV, or to drive a POV on official business and/or to use Government-issued electronic equipment.
- (c) The provisions of this policy shall not apply to the following:
 - (1) Emergency use of a mobile telephone, including calls to 911 or 311, a hospital, an ambulance service provider, a fire department, a law enforcement agency, or a first-aid squad;
 - (2) Use of a mobile telephone by law enforcement and emergency personnel or by a driver of an authorized emergency vehicle, acting within the scope of official duties;
 - (3) Initiating or terminating a telephone call, or turning the telephone on or off;
 - (4) Inputting and changing various frequencies or direction finding data while on official business and driving government-provided Direction Finding Vehicles; or
 - (5) Other exigent circumstances deemed reasonable.

10. GENERAL PROVISIONS.

- (a) This Directive shall be implemented consistent with applicable law and subject to the availability of appropriations.
- (b) This Directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the FCC, its agencies or entities, its officers, employees or agents, or any other person.



Steven VanRoekel
Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Official Use of Social Media by FCC Bureaus, Offices, and Staff	
	Directive Number: FCCINST 1440.1	Effective Date: April 9, 2014

1. **PURPOSE:** This Directive sets forth the Federal Communication Commission’s (“Commission” or “FCC”) policies, procedures, and responsibilities relating to the official and authorized use of social media by FCC employees and contractors on behalf of the Commission.
2. **BACKGROUND:** The FCC is committed to using Social Media tools to create a more effective and transparent government, to engage practitioners, the public and other interested parties, and facilitate internal collaboration. Social Media provides a dynamic set of tools to help the FCC accomplish its objective to be a “responsive, efficient and effective agency capable of facing the technological and economic opportunities of the new millennium.”¹ Social Media use has been widely adopted as a means of making government “more efficient, effective and responsive to citizens’ needs.”²
3. **SCOPE AND APPLICABILITY:** This Directive applies to all Bureaus and Offices (B/Os) within the FCC. The policy and procedures outlined here apply to all Commission employees.
4. **DEFINITIONS:**

Branding. “Branding” refers to the use of a logo, seal, symbol, design, and/or name as part of activities to distinguish from those of non-FCC actors.

Employees. “Employees” refers to all Commission employees, including consultants, temporary employees, interns and contractors acting in an official capacity.

¹ See FCC What We Do webpage, available at <http://www.fcc.gov/what-we-do>

² See White House Open Government Initiative, available at <http://www.whitehouse.gov/open>

Social Media. “Social Media” is a broad term that encompasses a wide and evolving variety of interactive and user-driven content technologies (*i.e.*, social networks, blogs, wikis, podcasts, online videos, etc.).

Third-party websites or applications. The term “third-party websites or applications” refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernmental entity.

5. ROLES AND RESPONSIBILITIES:

- A. Office of Media Relations (“OMR”) is responsible for external communications on behalf of the FCC, including the content-related aspects of Social Media. Content-related coordination on Social Media will occur among OMR representatives working with the Bureaus and Offices. OMR is responsible for identifying categories of content and the associated approval process. OMR is the final decision-maker for sensitive content that requires approval. OMR, or its designated staff, is responsible for creating content schedules, developing messages for social media distribution, and handling comment moderation on applicable Social Media tools.
- B. FCC Information Technology (“FCC IT”) is responsible for FCC’s Information Technology related to Social Media, including privacy, security, tools, and technological resources needed to successfully operate in the Social Media space.
- C. Office of General Counsel (“OGC”) is responsible for providing legal advice and counsel on issues relating to FCC use of Social Media.
- D. Office of the Managing Director (“OMD”) is responsible for the administration and management of the Commission including the Commission's budget and financial programs; human resources; contracts and purchasing; communications and computer services (including FCC IT); physical space; security; the Commission meeting schedule; and distribution of official FCC documents.
- E. Bureaus and Offices (“B/Os”) all B/Os are responsible for designating a Social Media liaison to work with OMR to coordinate with regarding Social Media requests, content clearance and responses to questions received on Social Media. While all staff members can submit content for Social Media distribution, the B/O designee will coordinate and obtain content approval on an as-needed basis. All B/O supervisors have a duty to ensure that FCC’s use of social media is focused and mission-oriented.

6. POLICY:

The Commission encourages the use of Social Media technologies to enhance communication, transparency, collaboration, and information exchange in support of its mission³ and Open Government.⁴

FCC personnel are encouraged to access and contribute content for distribution on FCC's Social Media tools.

When utilizing social media in an official capacity, FCC employees shall abide by the "Guiding Principles for Official Use of Social Media," set forth below in Section 7 and the rules outlined and agreed upon in the "FCC Information Technology Rules of Behavior".

Except as provided in 5 CFR 2635.702(c), employees may not use their government position, title, or any authority associated with their public office or employment to endorse any product, service, or enterprise when using FCC Social Media tools in their official capacity.

7. Requirements and Policies Governing Official Use of Social Media:

Employees seeking to use Social Media for official use should coordinate with OMR and, as appropriate, OGC, OMD, and FCC IT and others specified below, to ensure that the use complies with applicable federal laws, regulations, and requirements, as well as Commission policies.

A. Potentially Sensitive Information

- i. Confidentiality/privileged information. Employees should be cautious not to unintentionally release confidential or privileged information concerning, for example, a pending proceeding (when such information is non-public), ongoing policy issues, or personally identifiable information, in accordance with the policies set forth in the FCC's Rules of Behavior and Standards of Ethical Conduct for Employees of the Executive Branch,⁵ as well as the Commission's rules regarding employee responsibilities and conduct that are codified in Part 19 of its rules, 47 C.F.R. § Part 19.⁶

³ See FCC What We Do webpage, *available at* <http://www.fcc.gov/what-we-do>

⁴ See White House Open Government Directive, *available at* <http://www.whitehouse.gov/open/documents/open-government-directive>

⁵ See FCC Computer System User Rules of Behavior, *available at* http://intranet.fcc.gov/docs/omd/itc/crc/tipsheets/Network/rules_of_behavior.pdf

⁶ This includes confidential commercial information that, if released, could be a criminal violation of the Trade Secrets Act, 18 U.S.C. § 1905.

- ii. Personally Identifiable Information (PII)/Information collection. If information is collected through the FCC's use of a third-party website or application, the FCC shall collect only the information necessary for the proper performance of agency functions. If PII is collected, the FCC shall collect only the minimum necessary to accomplish a purpose required by statute, regulation, or executive order.⁷

B. Third Party Websites/Applications

- i. Terms of Service. FCC will only use third-party websites and applications that have been approved by OMR and OMD for Agency use, and such use must be in accordance with approved Federal Terms of Service ("ToS") agreements negotiated by the General Services Administration ("GSA") or approved by OGC.⁸ Potential security and procurement issues associated with new tools will be addressed through the existing FCC procurement and security review processes.
- ii. Privacy Policies of third party websites. FCC is committed to protecting the privacy of its social media visitors. As a default, FCC will adhere to the privacy policies outlined in the third party website's Terms of Service (ToS) agreement, unless otherwise stated and officially amended. When privacy is not addressed in a ToS agreement, FCC will adhere to the FCC Privacy Policy.⁹
- iii. Embedded applications/Cyber Security Policy. If the FCC incorporates or embeds a third-party application on its website or any other official government domain, it shall take the necessary steps to disclose the third party's involvement and ensure activity is consistent with the Commission's Cyber Security Policy.¹⁰
- iv. Agency branding. In general, when the FCC uses a third-party website or application that is not part of an official government domain, it shall apply appropriate branding to distinguish its activities from those of nongovernment actors. For example, to the extent practicable, the FCC should add its seal or

⁷ See Memo for The Heads of Executive Departments and Agencies, Subject: Social Media, Web-based Interactive Technologies, and the Paperwork Reduction Act, *available at* http://www.whitehouse.gov/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf; *see also* Memo for The Heads of Executive Departments and Agencies, Subject: Guidance for Agency Use of Third-Party Websites and Applications, *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf

⁸ See listing of Federal-wide TOS agreements, *available at* <http://www.howto.gov/web-content/resources/tools/terms-of-service-agreements/negotiated-terms-of-service-agreements>

⁹ See FCC Privacy Policy, *available at* <http://www.fcc.gov/encyclopedia/privacy-policy>

¹⁰ See FCC Directive FCCINST 1479.4 Cyber Security Program, *available at* <http://intranet.fcc.gov/docs/omd/perm/directives/1479.4.pdf>; *see also* Guidelines for Secure Use of Social Media by Federal Departments and Agencies, *available at* https://cio.gov/wp-content/uploads/downloads/2012/09/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

emblem to its profile page on a social media website to indicate that it is an official agency presence. Whenever possible, accounts on Social Media sites should be identified by using the Commission's full name (the Federal Communications Commission), and where appropriate, a link to www.fcc.gov.

C. Other Issues

- i. OMR Issues: Employees should contact OMR with general questions about requirements and policies covered in this Directive.
- ii. OMD and FCC IT Issues: Employees should contact OMD with questions about Privacy, Procurement, Information Security, and Federal Records Management.
- iii. FCC IT Issues: Employees should contact FCC IT with questions about technology-related to Social Media tools and other FCC information systems.¹¹
- iv. OGC Issues: Employees should contact OGC with questions about ex parte, copyright/fair use, or financial disclosure issues.

8. CONTRIBUTING TO THE COMMISSION SOCIAL MEDIA ACCOUNTS:

- A. New Social Media Accounts. As a general practice, the Commission will only have one account for any given Social Media tool (e.g. FCC will only have one Facebook page). This is to ensure the Commission is communicating in a unified voice, adhering to its Social Media policies and procedures, maximizing reach by not fragmenting audiences across different pages, and making the most efficient and effective use of the resources available to maintain the Commission's Social Media presence.¹²
- B. Content Types (including "likes", "follows", "shares", and retweets ("RT")). The FCC will utilize Social Media to advance the FCC's mission. In addition to promoting content developed by the FCC, the FCC may share industry-related content from a variety of sources, including Government, commercial and nonprofit telecommunication organizations, consistent with applicable intellectual property laws. If and when the FCC shares third party content, attribution will be given to the originating content owner, which may include but is not limited to "tagging" the content owner's Social Media account.

The FCC may "follow" and/or "like" any Social Media page that has relevant content, including other government entities, commercial businesses and nonprofit

¹¹ The Consumer and Governmental Affairs Bureau (CGB), with support from FCC IT, will handle Section 508 issues. Employees should contact CGB with questions regarding Section 508.

¹² Excludes FCC Chair, Commissioners and certain approved senior-level positions.

organizations. OMR is responsible for implementing official decisions to “like” and “follow” accounts.

The FCC does not endorse any product or service, nor can it guarantee the validity or timeliness of the content posted by commenters outside of the FCC onto the official FCC Social Media page. All of FCC’s Official Social Media pages must include the disclaimer that “likes,” “follows” and “shares” do not imply endorsement.

9. PROCEDURES FOR CREATING NEW SOCIAL MEDIA ACCOUNTS AND SUBMITTING CONTENT FOR DISTRIBUTION AND CLEARANCE:

A. New Account Requests. Any and all requests for new Social Media accounts (whether FCC already has an established presence or not) should be made via email to SocialMedia@fcc.gov. In your request please include the following elements:

- Tool: Identify the tool requested
- Bureau/Office: Identify the Bureau/Office submitting the request
- Justification: Provide a brief justification on why this tool is needed, how this tool will meet that need, and why other Social Media channels already in use will not suffice
- Resources: Available resources your Bureau/Office has to maintain or manage presence
- Cost: Identify any costs associated with proposed tool

OMR, in conjunction with appropriate FCC management officials, will make a determination on each Social Media request.

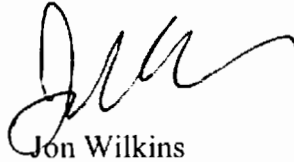
B. Submitting Content for Social Media Distribution. All requests for content promotion across FCC Social Media tools should be sent to SocialMedia@FCC.gov with the following information:

- Bureau/Office: Identify the Bureau/Office submitting the request
- Description: Provide a brief description of material to be promoted
- URL: Will content related to Social Media request be available on FCC.gov?
- Date: Provide any dates associated with this request
- Public Information: Whether the content associated with the request is appropriate for public distribution

C. Content Clearance. As needed, OMR will work with OGC, OMD, FCC IT, other B/Os, and the Office of the Chairman to review content prior to public distribution to ensure:

- Alignment with Commission priorities
- Coordination with other communication channels
- Proper Disposition of Sensitive information

After the initial review, OMR will determine whether additional content review is needed. If additional review is needed, OMR will follow up directly with the designated point of contact for the proposed Social Media content.

A handwritten signature in black ink, appearing to read 'Jon Wilkins', with a stylized, cursive script.

Jon Wilkins
Acting Managing Director

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Compliance with the FCC Cyber Security Program	
	Directive Number: FCCINST 1479.5	Effective Date: May 20, 2015

TO: All Employees

SUBJECT: Compliance with the FCC Cyber Security Program

Purpose. This directive establishes policy and assigns responsibilities for assuring optimal levels of cyber protection required for Federal Communications Commission (FCC) information systems. This Directive also authorizes issuance of the *FCC Cyber Security Policy* program which containing detailed policies, procedures, and information requirements for implementing cyber security controls. The *FCC Cyber Security Policy* will be updated, as necessary, to reflect changes in law, regulation or Presidential guidance or Executive Order.

Scope. This Directive applies to all FCC Bureaus, Offices, and Staff including Federal employees, contractors, temporary staff, interns, and volunteers who access and use FCC information systems to conduct the Commission's business including remote access and use such as while teleworking or on travel.

Authorities. This Directive is covered by numerous Public Laws, Executive Orders, regulations, Presidential Decision Directives, OMB Circulars, and National Institute of Standards and Technology publications among other guidance and authoritative references. A complete and detailed list is located in Appendix C of the *FCC Cyber Security Policy*.

Policy. The FCC's cyber mission is to ensure the security of our information resources, environment and communications to provide a secure, reliable, and resilient platform where both the Commission and the public can access information. The Commission increasingly relies on information technology, specifically the internet, wireless and mobile devices, and data exchange services to conduct its business. Cyber security measures are crucial to ensure the protection and preservation of the confidentiality, integrity, and availability of electronic information resources critical to the FCC, the U.S. Government, and the public.

The *FCC Cyber Security Policy*, incorporated by reference into this Directive, comprises the cyber security management structure and foundation to measure progress and compliance, and is organized into five major sections as follows:

SECTION 1: INTRODUCTION -- This section covers among other items, the information security program, the policy overview, various cyber threats and information technology definitions.

SECTION 2: ROLES and RESPONSIBILITIES -- This sections covers in detail the roles and responsibilities of information security staff, organizations and individuals ranging from the Chairman's position to individual users as addressed under Scope above.

SECTION 3: MANAGEMENT CONTROLS -- These controls focus on managing both system information security controls and system risk. These controls consist of risk mitigation techniques used by management.

SECTION 4: OPERATIONAL CONTROLS -- These controls focus on mechanisms primarily implemented and executed by individuals. Operational controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.

SECTION 5: TECHNICAL CONTROLS -- These controls focus on security controls executed by information systems. Technical controls provide automated protection from unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data.

Responsibilities.

Listed below are the major responsibilities for the key positions that oversee FCC information security. A complete list of roles and responsibilities for all information security levels are located in Section 2 of the *FCC Cyber Security Policy* document.

- A. The Managing Director is responsible for oversight of the cyber security program and allocation of adequate resources for information system security and shall:
- Appoint the Chief Information Officer (CIO);
 - Ensure that an Cyber Security Program is established and managed in accordance with Federal law, regulation, directives and order, and by FCC policy and directives;
 - Ensure that Senior officials such as the CIO, Deputy CIO for Resiliency (DCIOR) and Chief Information Security Officer (CISO) are held accountable for data and information systems protection;
 - Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained;
 - Ensure that adequate funding for information security is provided for information

systems and that adequate funding requirements are included for all information systems budgets;

- Ensure that information system data are entered into the appropriate FCC Security Management Tools to support FCC information security oversight and FISMA reporting requirements; and
- Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported.

B. The Chief Information Officer is the senior agency executive responsible for all FCC information systems and their security as well as for ensuring FISMA compliance and shall:

- Heads an office with the mission and resources to assist in ensuring compliance with the FCC Information Security Program;
- Oversees the development and maintenance of a Commission-wide information security program;
- Appoints a FCC employee to serve as the DCIOR;
- Appoints a FCC employee to serve as the CISO;
- As appropriate, serves as or appoints a FCC employee to serve as the Authorizing Official (AO) for FCC information systems.
- Participates in developing FCC performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the FCC security program;
- Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with FCC information security policies;
- Ensures that FCC security programs integrate fully into the FCC enterprise architecture and capital planning and investment control processes;
- Ensures that System Owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control;
- Reviews and evaluates the FCC Cyber Security Program annually;
- Ensures that an information security performance metrics program is developed, implemented, and funded;
- Reports to the FCC Managing Director on matters relating to the security of FCC systems;
- Ensures compliance with applicable information security requirements;
- Coordinates and advocates resources for enterprise security solutions; and
- Leads the FCC Contingency Planning program.

C. The Deputy Chief Information Officer for Resiliency is responsible for all commission information systems and their security as well as for ensuring FISMA compliance and shall:

- Establish and oversee the FCC information security program;
- Direct a review of the information security program plan be performed with a frequency depending on risk, but no less than annually;
- Ensure that information security concerns are addressed at Configuration Control Boards, and throughout the System Development Life Cycle
- Ensure that an accurate information systems inventory is established and maintained;
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with FCC information security policies
- Ensure that System Owners understand and appropriately address risks, including risks arising from interconnectivity with other programs and systems outside their control;
- Ensure that an information security performance metrics program is developed, implemented, and funded;
- Advise the FCC CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern;
- Ensure that incidents are reported to the Network Security Operations Center (NSOC) within reporting time requirements as defined in *FCC Cyber Security Policy* document;
- Ensure compliance with FCC information systems security policy;
- Coordinate and advocate resources for information security enterprise solutions; and
- Provide the resources and qualified personnel to ensure compliance with FCC security policy.

D. The Chief Information Security Officer is responsible for developing a security strategy and establishing, maintaining, directing and coordinating implementation of the FCC Cyber Security program and shall:

- Ensure that appropriate technical, management, and operational controls are in place for adequately protecting FCC data and information systems, including data stored or used when remotely such as teleworking or traveling on official business;
- Establish a Cyber Security Program that addresses federal statutory and regulatory requirements for the high-level areas;

- Issue agency-wide cyber security policy, guidance, and security architecture requirements for all FCC IT systems and networks, in compliance with the authorities listed in Appendix C of the *FCC Cyber Security Policy* document;
 - Serve as the principal agency liaison with organizations outside the FCC for matters relating to cyber security;
 - Review and approve the tools, techniques, and methodologies planned for use in applying the Risk Management Framework to FCC IT systems and for reporting and managing systems-level FISMA data, including but not limited to Security Test and Evaluation (ST&E) plans, contingency plans, and security risk assessments;
 - Consult with the FCC Chief Security Officer on matters pertaining to physical security, personnel security, investigations, and Top Secret (TS) and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure;
 - Develop and implement procedures for detecting, reporting, and responding to information security incidents;
 - Consult with the Office of General Counsel, Office of the Inspector General, and the Office of Managing Director's Human Resources Management to develop and/or update the FCC Computer System User Rules of Behavior (RoB). Work with OMD's Human Resources Management, the Security Operations Center and the Enterprise Acquisition Center, and B/Os to ensure all users read and sign indicating acceptance of the RoB;
 - Ensure that all individuals receive security awareness training BEFORE accessing and using the FCC network and information systems;
 - Provide oversight and guidance for the FCC Network Security Operations Center (NSOC); and
 - Consult with the International Bureau regarding cyber security matters involving international travel and travelers on official FCC business.
- E. The System Owners or Technical Stewards are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. All systems require a System Owner designated in writing for proper administration of security and shall:
- Ensure that each of their systems is deployed and operated in accordance with the *FCC Cyber Security Policy* document;
 - Ensure that an Information System Security Officer (ISSO) is designated in writing for each information system under their purview;

- Ensure only one System Owner designated for each FCC system;
- Ensure information security compliance, development and maintenance of security plans, user security training (if applicable), notifying officials of the need for security authorization and need to resource; and
- Ensure development of a POA&M to address weaknesses and deficiencies in the information system and its operating environment.

F. All Individuals that access and use the FCC network and information systems shall read, sign and follow the FCC Computer User Rules of Behavior.



Jon Wilkins
Managing Director