



governmentattic.org

"Rummaging in the government's attic"

Description of document:	National Capital Planning Commission (NCPC) Succession Plan and National Security Classified Information Policy, 2012
Requested date:	18-February-2016
Released date:	23-February-2016
Posted date:	27-June-2016
Source of document:	National Capital Planning Commission Attn: Chief FOIA Officer 401 9th Street, NW North Lobby, Suite 500 Washington, D.C. 20004 Fax: 202-482-7272 Email: anne.schuyler@ncpc.gov

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.

February 23, 2016

Copy by Electronic Mail

I am writing in response to your Freedom of Information Act request to the National Capital Planning Commission ("NCPC") dated February 18, 2016 and received in this office on February 18, 2016.

In your letter you request a copy of NCPC's Succession Plan and a copy of NCPC's current National Security Classified Information Policy.

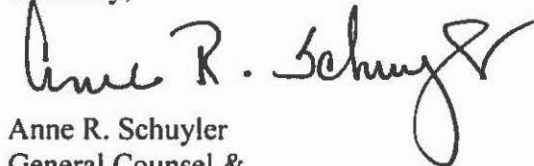
In response to your request, I am attaching both requested documents to the e-mail conveying this letter.

There is no charge associated with this request because it took less than two hours of search time and information was provided electronically which required no duplication.

This determination may be appealed administratively within sixty days of the date of this letter by writing to the Chairman, National Capital Planning Commission, 401 9th Street, NW, North Lobby 5th Floor, Washington, D.C. 20004. You should clearly mark your envelope and letter: "Freedom of Information Appeal." Be advised the NCPC adopted new FOIA regulations effective March 31, 2014, and a copy of the new regulations may be accessed at www.ncpc.gov.

If you need any further assistance, please contact me at the above address or you may reach me at (202) 482-7223.

Sincerely,



Anne R. Schuyler
General Counsel &
Chief FOIA Officer

Attachments

Succession Management Framework

National Capital Planning Commission

**Prepared and Maintained By:
Office of Administration
401 9th Street, NW
Suite 500
Washington, DC 20004**

OUR MISSION

We are the central planning agency for the federal government in Washington, D.C. and the counties of Prince George's and Montgomery in Maryland; Arlington, Fairfax, Prince William, and Loudoun in Virginia, plus the independent cities and towns within the outer boundaries of these counties. We develop plans and review development proposals that enhance the National Capital's extraordinary historical, cultural, and natural resources. Our long-range plans anticipate the needs of the federal establishment well into the 21st century, while our shorter-term initiatives proactively address its more immediate requirements. We conduct research to provide practical information to federal and local decision makers needed to formulate development policy in the National Capital Region (NCR). We partner with other federal agencies, local governments, private organizations, and citizens to create a more beautiful and livable capital.

OUR VISION

We aspire to creative and visionary planning, building on the nation's rich cultural heritage and carrying forward the legacy of historic plans to inspire generations, now and in the future, to achieve the world's most magnificent capital. We are committed to ensuring that development in the Nation's Capital meets the highest standards of design and planning excellence. We endeavor to serve as a resource for the latest planning information and state-of-the-art technology applications and generate useful data and analysis on land use, demographic, and related economic issues in the region. Our goal is to provide critical information and guidance to decision-makers and citizens as they consider the design and funding of development plans and policies for the Nation's Capital.

OUR VALUES

As public servants dedicated to excellence, our emphasis is on providing high quality professional service to our customers - the citizens of Washington, D. C., the National Capital Region (NCR) and the United States. We are competent professionals who strive to provide service that is effective, efficient, responsive, and reliable. Excellent service is the standard by which the Commission's effectiveness and efficiency is measured. Improvement in performance comes from our vision-driven focus on those we serve. We aspire to be creative and visionary in our day-to-day activities and to try to reflect in our work, and professional relationships the ideals and principles which are so eloquently represented in the historic plans and symbols that we are tasked to preserve.

COOPERATION: We seek to forge effective partnerships with federal and local agencies, professional and civic organizations, and members of the public to achieve shared objectives that improve the quality of life and safety of those who live, work, and visit in the Nation's Capital.

OPENNESS: We strive to disseminate full, clear, and accurate information on planning and urban design issues to citizens to encourage their participation in the planning process and provide a widely accessible public forum for members of the public to express their views on planning matters in the region.

CREATIVITY: We are forward-thinking advocates of community design and renewal, and we seek innovative solutions to local and federal government needs.

LEADERSHIP: We aspire to a leadership role in the local, national, and international planning community by maintaining high levels of expertise and proficiency in our professional fields. We will lead by example, educating and informing all citizens and employing cutting-edge practices and technologies.

SERVICE: We are results-oriented public servants dedicated to excellence and hold ourselves accountable for both the immediate needs of the federal establishment and the long-range consequences of our present actions.

TRUST: We endeavor to protect the integrity of the National Capital's built and natural environment and serve as effective stewards in preserving Washington's extraordinary planning legacy.

THE VALUE OF SUCCESSION PLANNING

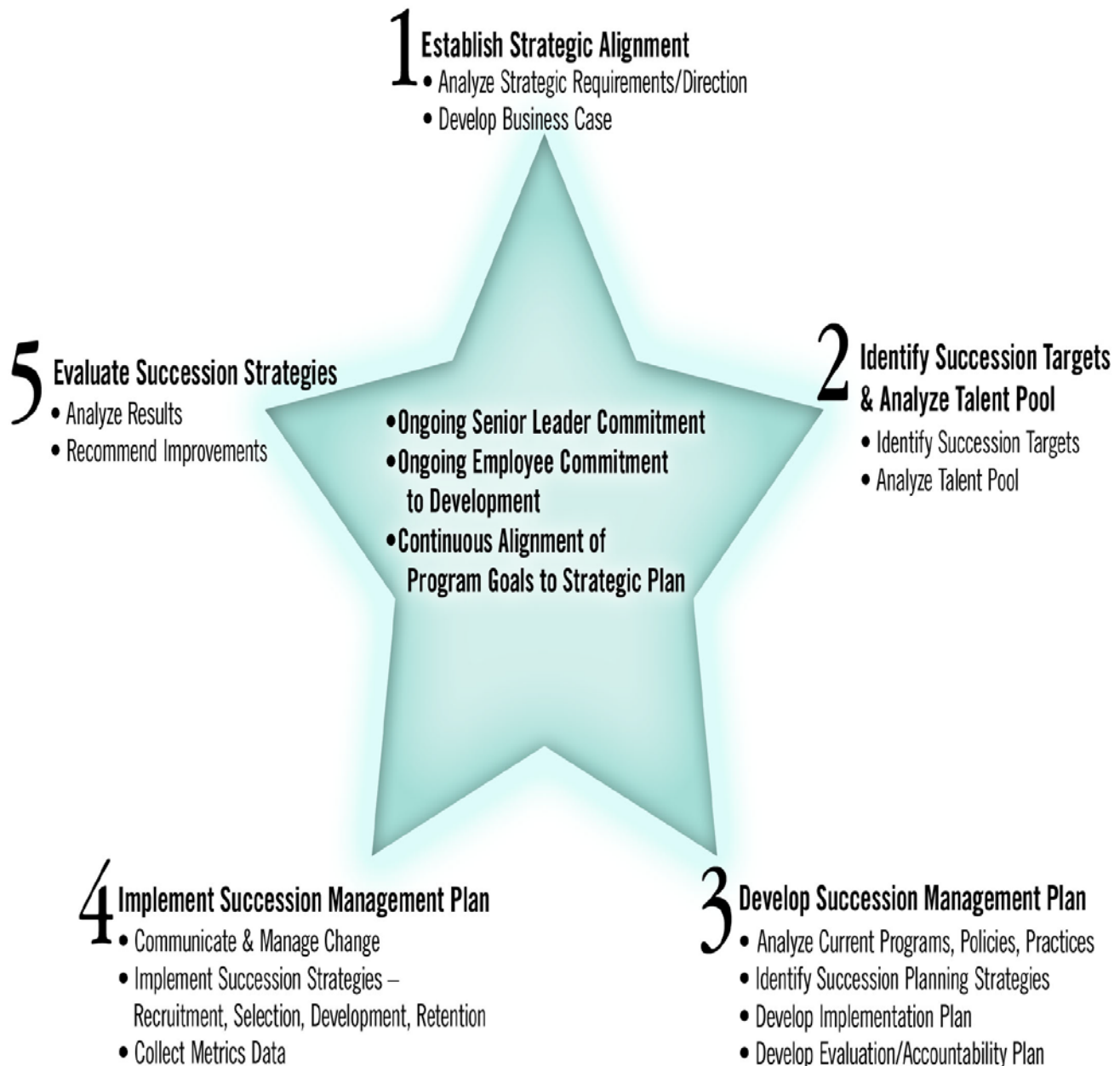
Succession management is a systematic approach to ensuring a continuous supply of the best talent through helping individuals develop potential. The achievement of the Commission's goals is based on funding and staffing levels remaining stable and minimal changes by external forces and/or parties. As the number of employees eligible for retirement rises, it is important to have a plan in place to insure that there is a pool of qualified internal applicants ready to be considered for a key leadership position.

Continuity of leadership is also important to ensure that the National Capital Planning Commission (NCPC) can strive to reach its Human Capital goals as stated in NCPC's Annual Performance Plan, which was developed as part of NCPC's Strategic Plan. This Plan is grounded in reality, and focused on results, as required by the Government Performance and Results Act (Public Law 103-62).

Because NCPC feels strongly about the need to conduct succession planning, senior management has committed multiple resources to ensure its success, including funds for formal leadership development programs (\$10,000 - \$15,000 per year), work time for employees to participate in developmental opportunities, and other internal developmental opportunities. Internal and external development opportunities will be further described under "Succession Planning Strategies".

SUCCESSION PLANNING MODEL

NCPC plans to use the succession planning model below provided by the Office of Personnel Management (OPM):



WORKFORCE ANALYSIS

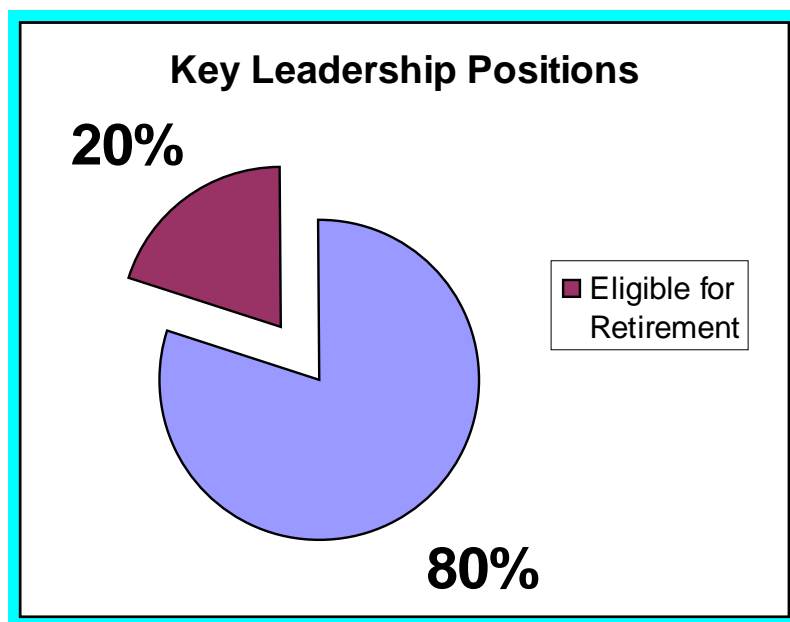
NCPC has identified the following positions as part of their key leadership population:

- Executive Director
- Chief Operating Officer
- Supervisory Community Planner
- Supervisory Architect (Urban Design)
- General Counsel
- Supervisory Public Affairs Specialist
- Executive Assistant (Secretariat) / Administrative Officer

The above positions have been identified as mission critical and therefore the continuity of leaders in these positions is essential to achieving NCPC's strategic goals.

NCPC plans to complete additional workforce analyses to identify historical data, trends and projected attrition to evaluate and prioritize future needs and vacancies in their key leadership population. The results from this analysis along with other key pieces of information will form the basis for formulating specific strategies, action plans, and initiatives that will support the agency's succession plan.

Eligibility for retirement of employees in key leadership positions is represented in the chart below. The 20% eligible for retirement will reach retirement status in the next 5 years. The development of the succession plan will facilitate an easy transition when employees choose to retire.



LEADERSHIP COMPETENCY ASSESSMENT

A leadership competency assessment will be conducted based on OPM's leadership model.

OPM LEADERSHIP COMPETENCIES		
Leading Change	<ul style="list-style-type: none"> . Flexibility . Resilience . Service Motivation . Continual Learning 	<ul style="list-style-type: none"> . Creativity/Innovation . Vision . External Awareness . Strategic Thinking
Leading People	<ul style="list-style-type: none"> . Integrity/Honesty . Cultural Awareness 	<ul style="list-style-type: none"> . Conflict Management . Team Building
Building Coalitions/Communications	<ul style="list-style-type: none"> . Oral Communication . Written Communication . Interpersonal Skills 	<ul style="list-style-type: none"> . Influencing/Negotiating . Partnering . Political Savvy
Results Driven	<ul style="list-style-type: none"> . Decisiveness . Customer Service . Technical Credibility 	<ul style="list-style-type: none"> . Problem Solving . Accountability . Entrepreneurship
Business Acumen	<ul style="list-style-type: none"> . Human Resources Management . Financial Management . Technology Management 	<ul style="list-style-type: none"> . Contract Management

In addition to assessing the leadership competencies, critical technical skills will also be assessed. Key leadership positions & relevant critical technical competencies are identified in the table below.

Leadership Position	Critical Competencies
Executive Director	<ul style="list-style-type: none"> . Expert Knowledge of planning concepts, principles, techniques and practices . Ability to identify community needs, resources and problems
	<ul style="list-style-type: none"> . Expert Knowledge of planning concepts, principles, techniques and practices
Chief Operating Officer	<ul style="list-style-type: none"> . Expert knowledge of contract administration and procurement . Comprehensive knowledge of space and property management . Expert knowledge of budget and financial management.
Supervisory Community Planner	<ul style="list-style-type: none"> . Mastery of planning principles and practices
Senior Architect	<ul style="list-style-type: none"> . Mastery of architectural, urban design and planning principles and practices
General Counsel	<ul style="list-style-type: none"> . Knowledge of contract law, civilian personnel law, Freedom of Information Act, Privacy Act, standards of conduct and general administrative law . Ability to conduct and direct complex legal research, engage in sound legal analysis, and present results in a clear, precise and persuasive manner
Supervisory Community Planner	<ul style="list-style-type: none"> . Ability to effectively coordinate with all federal, state, and local government officials; business and civilian organizations; Congress and Administration; and members of general public on a wide variety of planning related issues . Ability to analyze programs & determine the most effective techniques to be used in reaching general and specialized audiences. . Skill as a principal spokesperson with representatives of all types of media
Executive Assistant (Secretariat)/ Administrative Officer	<ul style="list-style-type: none"> . Expert knowledge of overall goals, objectives, and mission of the Commission . Knowledge of events and milestones as it relates to project plan review, Commission proceedings, and the Executive Director Recommendation (EDR) preparation process . Mastery of the concepts, principles, practices, laws and regulations which

apply to budgeting and financial management.
.Knowledge of human resources, procurement, contracting, space management and information technology.

TALENT POOLS

Having a source of qualified candidates available to fill vacancies in a minimal amount of time is critical to leadership continuity. NCPC has identified internal and external talent pools to draw from for each position covered under the Agency's Succession Plan. The table below identifies each position and the talent pool that NCPC plans to tap into as vacancies arise.

Key Leadership Position	Internal Talent Pool	External Talent Pool
Executive Director, and Chief Operating Officer	Division Directors	City Government, American Planning Association, Newspapers, and USAJOBS.
Supervisory Community Planner, Supervisory Architect, General Counsel, Supervisory Public Affairs Specialist, and Executive Assistant (Secretariat)	Grade 13/14 employees	City Government, Outreach Programs, American Planning Association, Newspapers, and USAJOBS.

SUCCESSION PLANNING STRATEGIES

Organizations with effective succession planning efforts have common characteristics. One of those characteristics is the use of a variety of strategies that help build the continuity of talent needed for future succession.

NCPC is currently using and/or plans to use the succession planning strategies indicated in the table below. Once a workforce analysis and leadership competency assessment has been completed, NCPC will reevaluate the following strategies and any relevant programs, policies and/or practices to determine if additional strategies need to be implemented to close any identified competency gaps.

Strategy/Description	Currently Uses	Plans to Use
Job Rotations	Yes	
Formal Training: FEI and Harvard Courses	Previously used	Yes
Special Assignments	Yes	
Reflecting on Experience: Commission debrief	Yes	
Coaching and Counseling	Yes	
Mentoring	Yes, Informally	Creating a formalized program
Learning Groups – Brown Bag Lunches	Yes	
Recruitment	Yes	
IDP	Yes	

The National Capital Planning Commission would like to highlight a strategy already established, the Student Volunteer Services Program. This program is committed to providing student interns with valuable, substantive work experiences related to their academic courses of study. The program is designed to help the students grow academically, professionally, and personally. The primary goals are as follows:

- Strengthen the relationship between the work of educators and the occupational needs of the NCPC and the involved students.
- Expose the students to the working world so they can make realistic career choices.
- Acquaint students with the functions and operations of the NCPC.
- Provide the NCPC contacts with faculty and students to improve NCPC's recruitment efforts for new staff.

NCPC will use this strategy in combination with the strategies in the chart above to help build talent for the future needs of the agency.

IMPLEMENTATION STRATEGIES

NCPC is confident that it will continue to improve the skills of its current leadership and develop a leadership talent pool that is diverse and viable. The implementation of the succession management strategies will occur in stages. The first two stages have sequential timeframes. The third stage, Evaluation, overlaps with the first two stages, because baseline data may be collected during pre-rollout, and process and results metrics data may be collected during rollout and beyond.

Stage	Major Activities
PRE-ROLLOUT (Awareness)	<input type="checkbox"/> Determine an appropriate message <input type="checkbox"/> Develop communication materials <input type="checkbox"/> Develop employee tools and aids <input type="checkbox"/> Continue to integrate with existing programs <input type="checkbox"/> Develop succession strategies <input type="checkbox"/> Begin publicizing the succession management program
ROLLOUT (Activation and Commitment)	<input type="checkbox"/> Implement new succession strategies for recruitment, selection, development, and retention of agency leaders <input type="checkbox"/> Build elements of succession management into existing leadership courses and other activities, as appropriate <input type="checkbox"/> Collect data for metrics <input type="checkbox"/> Continue promoting succession management program <input type="checkbox"/> Brief supervisors on importance of succession management <input type="checkbox"/> Build enrollment in the succession management program
EVALUATION	<input type="checkbox"/> Gather data from existing sources <input type="checkbox"/> Develop new data sources <input type="checkbox"/> Prepare reports <input type="checkbox"/> Establish and implement ongoing evaluation process

The following table is provided to identify milestones and timelines with regards to succession planning activities.

Milestone	Planned Date of Completion
Identify plan/framework	
Workforce Analysis	
Pre-Rollout	
Leadership Competency Assessment	
Rollout	
Formalization of Mentoring Program	
Metrics	See chart for collection schedule
Succession Plan Evaluation	Annually

EVALUATION AND MONITORING PLAN

NCPC realizes the importance of measuring the effectiveness of all succession management programs and activities, including its approach for making continuous improvements and ensuring that succession targets and outcomes are realized. Training and development activities are a major component of succession management programs. Therefore, evaluating the effectiveness of training and development activities will be an integral component of the evaluation of the whole succession management program. The primary purpose of evaluation data is to make decisions. NCPC will evaluate the Agency's Succession Plan using a variety of criteria. Please refer to the metrics table in the appendix for a list of measures that will be used to evaluate NCPC's succession management program.

Accountability and evaluations are vital to ensure the effectiveness of the NCPC's succession plan and related programs. The Executive Director and the Chief Operating Officer will periodically and systematically evaluate the succession management program to ensure that intended outcomes are realized. Continuous improvements and feedback to top management and other responsible parties will occur on a regular basis. An extensive review will be completed annually, and improvements will be planned and implemented accordingly.

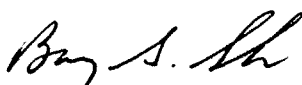
APPENDIX

Measure (may cover more than one objective)	Purpose	Measurement Approach	Frequency	Who Is Responsible
Employee satisfaction with leadership	To determine the extent to which employees hold their leadership in high regard, both overall and on specific facets of leadership	Employee survey	Annually	OA
Difference between competencies needed and competencies possessed by managers and leaders*	To determine the extent to which competency gaps are being closed for Management and Leadership Competencies	Assessment of competency gaps	Every 3 years	OA
Program compliance with merit system principles and related laws, rules, and regulations*	To determine that decision, policies, processes, and practices comply with merit system principles, and related laws, rules, and regulations governing Leadership Succession Management	<ul style="list-style-type: none"> Compliance assessment of programs: SES Candidate Development Program. And/or focus groups with leaders and employees. 	Incorporate into audit activities	Independent Audit Team
Percentage of corporate leadership positions filled from internal sources, other Government sources (including military) and non-Government sources	To determine the extent to which internal succession planning efforts result in the selection of leaders in corporate leadership positions	Data collected on recruitment sources when leaders are selected for corporate leadership positions	As positions are filled	
Average time from date vacancy announcement closes to date offer is made (expressed in working days) for corporate leadership positions	To determine the extent to which succession planning efforts are allowing the agency to fill corporate leadership positions in a timely manner	Data collected on time to hire	As positions are filled	
Bench Strength Index	To determine that plans are in place to mitigate corporate leadership succession risks	Any profile sheet that indicates that a corporate leadership position is at "high risk" must have an aggressive plan of action that addresses what will be done to reduce the risk rating	Semi-Annually	

MEMORANDUM

Date: April 3, 2012

To: NCPC Staff

From: Barry S. Socks 
Chief Operating Officer

Subject: National Security Classified Information Policy

Attached is NCPC's National Security Classified Information Policy. This policy applies to all offices of the Commission. All officials and employees who have current security clearances, and are required to have access to classified information or material in the performance of their assigned duties are required to understand this policy.

If you have any questions, please see me.

Attachment



NATIONAL CAPITAL PLANNING COMMISSION

NATIONAL SECURITY CLASSIFIED INFORMATION POLICY

APRIL 2012

NATIONAL SECURITY CLASSIFIED INFORMATION POLICY

1. Purpose

Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. This policy prescribes the procedures to be followed by National Capital Planning Commission (NCPC) employees who handle national security classified information, hereafter called "classified information.

2. Authorities

The Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) has the responsibility under Executive Order 13526 to develop, publish, and monitor policies pertaining to national security classified information. Individual agencies have the responsibility to implement ISOO policy through development of procedures within their agency. The requirements in this policy are based on the authorities of 46 C.F.R. § 503, E.O. 13526, and 32 C.F.R. § 2001 (E.O. 135265 Implementing Directive).

3. Scope

All NCPC employees with current security clearances are required to comply with the provisions of the policy.

4. Responsibility

The **Chief Operating Officer** is designated the Information Security Officer and Senior Agency Official with overall responsibility for:

- Implementing and maintaining the security program to meet the requirements of E.O. 13526, and 32 C.F.R. § 200; ensuring that the Commission's employment and retention of employees are consistent with national security interests and suitability requirements; and ensuring that security policies and procedures are developed, promulgated and implemented by appropriate officials.
- Initiating required personnel investigations and adjudicating those results which determine the suitability of employees requiring security clearances.
- Administering the Information Security Program under 46 C.F.R. § 503.51 et seq., E.O. 13526, and 32 C.F.R. § 2001 by:
 - (a) Determining whether an employee will be granted a security clearance, based upon the adjudication of results of required personnel investigations and the requisite "need to know."

(b) Briefing employees on their responsibilities for safeguarding national security information prior to receiving a security clearance and debriefing employees who no longer require a security clearance in accordance with Section 4.1(b) of E.O. 13526.

(c) Receiving, reviewing, and ensuring all classified information maintained within NCPC is properly secured and protected.

NCPC Employees with Security Clearances are responsible for:

- (a) Properly securing and protecting any classified information in their physical custody.
- (b) Reporting violations that result in the unauthorized disclosure of classified information.
- (c) Immediately notifying the Information Security Officer whenever classified information has been received by NCPC personnel for review.

5. Classified Information

Classified information is official information relating to our national defense or foreign relations that requires protection in the interest of national security. NCPC does not routinely handle classified information. However in rare instances, NCPC may have access to or receive classified information in its capacity as the central planning agency for the federal government in the National Capital Region. This information usually has been **originally** classified by an outside agency. On an infrequent basis, NCPC personnel may have a need to paraphrase or restate classified information. In doing so, the personnel must coordinate with the originating agency to avoid the unauthorized disclosure of classified information.

6. Levels of Classifications

Information is classified at one of three levels:

- **TOP SECRET** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- **SECRET** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

- **CONFIDENTIAL** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

7. Classification Authority

Original classification authority is specifically granted by the President or an official delegated that authority by the President. No official within NCPC has the authority to originally classify national security information. In any instance where an NCPC employee develops information that appears to warrant classification because of its relationship to the national defense or foreign relations of the United States, the material will be safeguarded in a manner consistent with this policy and transmitted to the Chief Operating Officer for further action.

8. Access to Classified Information

Access to classified information, orally, in writing, or by any other means, shall be limited to those persons whose official duties require knowledge or possession of an identified specific document, have received formal notification of access authorization, and have executed the "Classified Information Non-Disclosure Agreement" (SF-189 or SF-312). No one at the NCPC has a right to have access to classified information indiscriminately or solely by virtue of rank or position.

9. Clearances

A clearance is the formal authorization to access classified information. Following are the levels of clearances:

- **TOP SECRET** - access to information classified up to and including TOP SECRET.
- **SECRET** - access to information classified up to and including SECRET.
- **CONFIDENTIAL** - access to information classified up to and including CONFIDENTIAL.

10. Withdrawal of Clearance

The **Office Head** and/or the **Chief Operating Officer** may determine that a currently cleared employee no longer requires access to classified information in connection with the performance of official duties, and upon written notification to the holder, the Chief Operating Officer may administratively withdraw the access clearance. This withdrawal of an individual's access clearance is not an adverse or disciplinary action, and shall be without prejudice to the employee's eligibility for a clearance in the future.

11. Continuing Responsibility

Upon withdrawal or revocation of a clearance, the holder will be notified of the continuing responsibility to protect the information to which he/she previously had access.

12. Safeguards

Information classified under E.O. 13526, must be safeguarded against unauthorized disclosure in a manner that is commensurate with the sensitivity of the information. Classified information may not be removed from official premises without proper authorization. **The NCPC has no capability to handle classified information in an electronic environment. Therefore employees are not authorized to store, copy, scan or otherwise transmit classified national security information electronically at the NCPC .**

Cover Identification

Upon receipt of a national security classified document, the NCPC official will notify the ISO who must assign an appropriate cover sheet as the first page or cover of the document even if the document is only one page. The cover serves to quickly identify the document as classified, conceals the first page contents from casual observation, and warns unauthorized persons away from the document.

13. Storage

Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832. In addition, one of the supplemental controls below will be employed:

- (a) Inspection of the container every two hours by an employee cleared at least to the Secret level;
- (b) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of Intrusion Detection Equipment (IDE): All IDE must be in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the Chief Operating Officer; or
- (c) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF-L2740.

Secret information shall be stored in the same manner as Top Secret information or, until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock. Security-In-Depth is required in areas in which a non-GSA-approved container or open storage area is located. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required:

- (a) Inspection of the container or open storage area every four hours by an employee

cleared at least to the Secret level; or

(b) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

Combinations to dial-type locks shall be changed only by persons authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

- (a) Whenever such equipment is placed into use;
- (b) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or
- (c) Whenever a combination has been subject to possible unauthorized disclosure.

When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the combination lock should be reset to a standard combination of 50-25-50 for built-in combination locks or 10-20-30 for combination padlocks.

The neutralization and repair of GSA-approved security containers and vault doors will be in accordance with FED STD 809. The Director of ISOO will be notified when a violation occurs, under paragraphs 5.5(b)(1), (2), or (3) of E.O. 13526, that is reported to oversight committees in the legislative branch; may attract significant public attention; involves large amounts of classified information; or reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

14. Transmission

Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Guide.

Classified Information Transmitted Within the National Capital Planning Commission

All classified information transmitted within the agency will be prepared for transmission by placing it in a plain unmarked folder or envelope and transmitting it by hand through an authorized person to an authorized recipient. Classified material must not be sent in a U.S. Government Messenger Envelope (OF 658) or through the interoffice mail system.

Classified Information Transmitted to Another Office or Agency

All classified information transmitted to another office or agency must be enclosed in an opaque inner cover plainly marked with the assigned classification and addresses of both the sender and addressee. A receipt shall be attached to or enclosed in the inner cover which shall be sealed and addressed with no identification of the classification of its contents. All the seams of an envelope or wrapper must be sealed with tamper-resistant tape (e.g., fiber tape), plain brown postal tape, or packaged in a manner designed to provide tamper indication (e.g., by using security courier pouches) to prevent undetected access to the contents while in transit. The outer container must not bear any classification markings, list of contents, or any other information or marks that might indicate that the contents are classified. The outer container must show the complete, correct address of the recipient and the return address of the sender.

Containers to be delivered by messenger or courier must show complete street address and room number. The outer container may also be addressed to an individual; however, the concerns described in subpart 5.4b(3) of the NARA Security handbook should be taken into consideration before doing so. Primarily, office codes or phrases such as "Attention: Security Division" should be used.

TOP SECRET shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service.

SECRET information shall be transmitted by authorized messenger or by the United States Postal Service registered mail.

CONFIDENTIAL information shall be transmitted by authorized messenger or by the United States Postal Service certified, first class or express mail service. A commercial express mail delivery service for classified documents must not be used.

15. Sanctions and Penalties

NCPC employees with clearances are subject to appropriate sanctions if they:

- (a) Knowingly and willfully classify or continue the classification of information in violation of E.O. 13526, and 32 C.F.R. § 2001 or this Guide section;
- (b) Knowingly and willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 13526 or prior orders; or
- (c) Knowingly and willfully violate any provisions of E.O. 13526, and 32 C.F.R. § 2001, or this Guide section.

Sanctions may include reprimand, suspension without pay, removal, termination of access to classified information authority, or other sanctions in accordance with applicable law.

Criminal Penalties

Unauthorized disclosure of national security classified information may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, the provisions of Section 783(b) of Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982.

Reporting Unauthorized Disclosures or Attempts to Obtain Unauthorized Access to Classified Information

Employees must report unauthorized disclosures or attempts at unauthorized access of information to the Information Security Officer/Senior Agency Official who will conduct a preliminary investigation to ascertain the nature of the information disclosed and the extent of its dissemination, if any. The Federal Bureau of Investigation (FBI) investigates all instances in which actual attempts or actual unauthorized disclosures have been made.

16. Self-Inspections

The Chief Operating Officer will do an annual review of the program and report the results to the Executive Director.

17. Security Education and Training

The Chief Operating Officer shall:

- (a) Establish a Commission security education program to familiarize all personnel who have or may have access to classified information with the provisions of Executive Order 13526 and directives of 1500;
- (b) Initial training on basic security policies, principles, practices and criminal, civil and administrative penalties. Such training shall be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information;
- (c) Methods for the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information;
- (d) Establish controls to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons;
- (e) Act on all suggestions and complaints concerning the Commission's information security program; and

(f) Recommend appropriate administrative action to correct abuse or violations of any provision of Executive Order 13526.

18. Reporting Requirements

Each agency that creates or handles classified information is required to report annually to the Director of ISOO statistics related to its security classification program. The Chief Operating Officer shall prepare the SF-311 report, "Agency Security Classification Management Program Data" no later than November 15 each year.

Information on costs associated with the implementation of E.O. 13526 is required from each agency. The Human Resources Officer and Chief Operating Officer shall, in conjunction, prepare the "Report on Cost Estimates" no later than March 31st of each year.

19. Clearances

A clearance is the formal authorization to access classified information. Following are the levels of clearances:

- **TOP SECRET** - access to information classified up to and including TOP SECRET.
- **SECRET** - access to information classified up to and including SECRET.
- **CONFIDENTIAL** - access to information classified up to and including CONFIDENTIAL.

20. Withdrawal of Clearance

The **Office Head** and/or the **Chief Operating Officer** may determine that a currently cleared employee no longer requires access to classified information in connection with the performance of official duties, and upon written notification to the holder, the Chief Operating Officer may administratively withdraw the access clearance. This withdrawal of an individual's access clearance is not an adverse or disciplinary action, and shall be without prejudice to the employee's eligibility for a clearance in the future.

21. Continuing Responsibility

Upon withdrawal or revocation of a clearance, the holder will be notified of the continuing responsibility to protect the information to which he/she previously had access.

22. Safeguards

Information classified under E.O. 13526, must be safeguarded against unauthorized disclosure in a manner that is commensurate with the sensitivity of the information. Classified information may not be removed from official premises without proper

authorization. **The NCPC has no capability to handle classified information in an electronic environment. Therefore employees are not authorized to store, copy, and scan or otherwise transmit classified national security information electronically at the NCPC.**

23. Cover Identification

Upon receipt of a national security classified document, the NCPC official will notify the ISO who must assign an appropriate cover sheet as the first page or cover of the document even if the document is only one page. The cover serves to quickly identify the document as classified, conceals the first page contents from casual observation, and warns unauthorized persons away from the document.

24. Storage

Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832. In addition, one of the supplemental controls below will be employed:

(a) Inspection of the container every two hours by an employee cleared at least to the Secret level;

(b) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of Intrusion Detection Equipment (IDE): All IDE must be in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the Chief Operating Officer; or

(c) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF-L2740.

Secret information shall be stored in the same manner as Top Secret information or, until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock. Security-In-Depth is required in areas in which a non-GSA-approved container or open storage area is located. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required:

(a) Inspection of the container or open storage area every four hours by an employee cleared at least to the Secret level; or

(b) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

Combinations to dial-type locks shall be changed only by persons authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

- (a) Whenever such equipment is placed into use;
- (b) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or
- (c) Whenever a combination has been subject to possible unauthorized disclosure.

When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the combination lock should be reset to a standard combination of 50-25-50 for built-in combination locks or 10-20-30 for combination padlocks.

The neutralization and repair of GSA-approved security containers and vault doors will be in accordance with FED STD 809. The Director of ISOO will be notified when a violation occurs, under paragraphs 5.5(b)(1), (2), or (3) of E.O. 13526, that is reported to oversight committees in the legislative branch; may attract significant public attention; involves large amounts of classified information; or reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

25. Transmission

Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Guide.

Classified Information Transmitted Within the National Capital Planning Commission

All classified information transmitted within the agency will be prepared for transmission by placing it in a plain unmarked folder or envelope and transmitting it by hand through an authorized person to an authorized recipient. Classified material must not be sent in a U.S. Government Messenger Envelope (OF 658) or through the interoffice mail system.

Classified Information Transmitted to another Office or Agency

All classified information transmitted to another office or agency must be enclosed in an opaque inner cover plainly marked with the assigned classification and addresses of both the sender and addressee. A receipt shall be attached to or enclosed in the inner cover which shall be sealed and addressed with no identification of the classification of its

contents. All the seams of an envelope or wrapper must be sealed with tamper-resistant tape (e.g., fiber tape), plain brown postal tape, or packaged in a manner designed to provide tamper indication (e.g., by using security courier pouches) to prevent undetected access to the contents while in transit. The outer container must not bear any classification markings, list of contents, or any other information or marks that might indicate that the contents are classified. The outer container must show the complete, correct address of the recipient and the return address of the sender.

Containers to be delivered by messenger or courier must show complete street address and room number. The outer container may also be addressed to an individual; however, the concerns described in subpart 5.4b(3) of the NARA Security handbook should be taken into consideration before doing so. Primarily, office codes or phrases such as "Attention: Security Division" should be used.

TOP SECRET shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service.

SECRET information shall be transmitted by authorized messenger or by the United States Postal Service registered mail.

CONFIDENTIAL information shall be transmitted by authorized messenger or by the United States Postal Service certified, first class or express mail service. A commercial express mail delivery service for classified documents must not be used.

26. Sanctions and Penalties

NCPC employees with clearances are subject to appropriate sanctions if they:

- (a) Knowingly and willfully classify or continue the classification of information in violation of E.O. 13526, and 32 C.F.R. § 2001 or this Guide section;
- (b) Knowingly and willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 13526 or prior orders; or
- (c) Knowingly and willfully violate any provisions of E.O. 13526, and 32 C.F.R. § 2001, or this Guide section.

Sanctions may include reprimand, suspension without pay, removal, termination of access to classified information authority, or other sanctions in accordance with applicable law.

Criminal Penalties

Unauthorized disclosure of national security classified information may constitute a

violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, the provisions of Section 783(b) of Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982.

Reporting Unauthorized Disclosures or Attempts to Obtain Unauthorized Access to Classified Information

Employees must report unauthorized disclosures or attempts at unauthorized access of information to the Information Security Officer/Senior Agency Official who will conduct a preliminary investigation to ascertain the nature of the information disclosed and the extent of its dissemination, if any. The Federal Bureau of Investigation (FBI) investigates all instances in which actual attempts or actual unauthorized disclosures have been made.

27. Self-Inspections

The Chief Operating Officer will do an annual review of the program and report the results to the Executive Director.

28. Security Education and Training

The Chief Operating Officer shall:

- (a) Establish a Commission security education program to familiarize all personnel who have or may have access to classified information with the provisions of Executive Order 13526 and directives of 1500;
- (b) Initial training on basic security policies, principles, practices and criminal, civil and administrative penalties. Such training shall be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information;
- (c) Methods for the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information;
- (d) Establish controls to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons;
- (e) Act on all suggestions and complaints concerning the Commission's information security program; and
- (f) Recommend appropriate administrative action to correct abuse or violations of any provision of Executive Order 13526.

29. Reporting Requirements

Each agency that creates or handles classified information is required to report annually to

the Director of ISOO statistics related to its security classification program. The Chief Operating Officer shall prepare the SF-311 report, "Agency Security Classification Management Program Data" no later than November 15 each year.

Information on costs associated with the implementation of E.O. 13526 is required from each agency. The Human Resources Officer and Chief Operating Officer shall, in conjunction, prepare the "Report on Cost Estimates" no later than March 31st of each year.