Description of document:	List of National Geospatial-Intelligence Agency (NGA) Instructions, 2016
Requested date:	28-February-2016
Released date:	30-March-2016
Posted date:	16-July-2016
Source of document:	FOIA Request NGA FOIA Program Office National Geospatial-Intelligence Agency FOIA Requester Service Center 7500 GEOINT Drive, MS S01-EGM Springfield, Virginia 22150-7500 Fax: 571-558-3130 Email: FOIANGA@nga.mil The Public Access Link (PAL) Sign-in

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

NGA-2016-FOI-00034

MAY 05 2016

RE: Freedom of Information Act (FOIA) request #2016-FOI-00034

This letter is in response to your Freedom of Information Act (FOIA) request submitted to the National Geospatial-Intelligence Agency (NGA) dated March 2, 2016, in which you requested: "1. NGA Instruction 8470.2R8, NGA Instruction for Internet Usage; 2. NGA Instruction 8470.3R8, Use of Electronic Mail and Other Electronic Communications; 3. Policy Notice 8740.1 Police Notice for External Webmail Access for Personal use, 12 Aug 2011; 4. NGA Office of General Counsel, Political Activities, The Hatch Act: Election Campaigns Rules for NGA Employees."

After a careful review of the documents responsive to your request, National Geospatial-Intelligence Agency (NGA) subject matter experts have determined that the documents may be released in full.

Appeals to this determination should be made in writing within 60 calendar days from the date of this letter. In the appeal, you should reference FOIA case 2016-FOI-00034, detailing your reasons for reconsideration and include a copy of this letter. Your appeal should be mailed to the National Geospatial-Intelligence Agency, FOIA/Privacy Act Program Office, Mail Stop N81-SISCS, 7500 GEOINT Drive, Springfield, VA 22150.

If you have any questions or concerns regarding this request, please contact Tiffany Richardson, at (571) 557-4141 or via-email at FOIANGA@nga.mil.

Sincerely,

Claudia Williams
FOIA/PA Program Manager

4 Enclosures

1. DRAFT NGA Instruction 8470.2, NGA Instruction for Internet Usage (11 pages)
2. NGA Instruction 8470.3R8, Use of Electronic Mail and Other Electronic Communications (6 pages)

3. Policy Notice 8740.1 Police Notice for External Webmail Access for Personal use, 12 Aug 2011 (2 pages)
4. NGA Office of General Counsel, Political Activities, The Hatch Act: Election Campaigns Rules for NGA Employees (1 page)

National Geospatial-Intelligence Agency

INSTRUCTION

NUMBER 8470.2
5 April 2016
Click here to enter text.

CIO-T

SUBJECT: National Geospatial-Intelligence Agency (NGA) Instruction for Internet Usage

References: See Enclosure 1.

1. PURPOSE. This NGA Instruction implements and establishes policy in accordance with Reference (a) for the use of Internet-based capabilities (IbC). It assigns responsibilities for key NGA components and states the obligations of NGA personnel while accessing the Internet for official and unofficial (personal use) at any NGA location. This instruction supersedes NI 8470.2, "NGA Instruction for Internet Usage," 9 December 2009, and cancels Policy Notice 8470.1, "External Webmail Access for Personal Use", 12 August 2011.

2. APPLICABILITY. This Instruction applies to all personnel (government, military, contractor, any other non-Department of Defense (DoD) personnel with access to NGA computer networks). It applies to all personnel accessing NGA computer networks and IbC in support of official and unofficial NGA related activities.

3. DEFINITIONS. See Glossary.

4. POLICY. It is NGA policy to:

a. Provide access to the Internet for official and approved non-official activities.

b. Utilize the Internet for only official and approved on-official activities and protect NGA information and information resources.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. EFFECTIVE DATE. This Instruction is effective on the date of signature.

Douglas P. McGovern
Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," 11 September 2012
(b) DoD 5500.7-R, "Joint Ethics Regulation," August 1993 (incorporates change 7, 17 November 2011)
(c) NGA Directive (NGAD) 8231, "Cyber Defense Operations", 19 May 2015
(d) NGAD 8000, "Information Management and the Chief Information Officer (CIO)," 9 August 2013
(e) NGA Policy Notice 8470.1, "External Webmail Access for Personal Use", 12 August 2011 (hereby cancelled)
(f) NGA Instruction (NI) 8470.2R8, "NGA Instruction for Internet Usage", 9 December 2009 (hereby rescinded)
(g) NI 8470.3R8, "NGA Instruction for Use of Electronic Mail and Other Electronic Communications," 9 January 2006
(h) NI 8400.1R7, "NGA Instruction for Acquiring Information Technology Products", 29 January 2007
(i) CNSS Policy Number 22, "Information Assurance Risk Management for National Security Systems", January 2012
(j) NGAI 8251.1, "NGA Instruction for Ports, Protocols and Services Management (PPSM), TBD
(k) NI 5750.2R7, "NGA Instruction for the Freedom of Information Act Program," 7 August 2007
(l) NI 8900.4R5, "NGA Instruction for Intelligence Oversight," 30 March 2006
(m) NI 5500.11R4, "NGA Instruction for Standards of Conduct," 2 October 2008
(n) NI 5720.1R10, "NGA Instruction for Clearance for Public Release," 8 December 2008
(o) NGA Managed Attribution (MA) Concept of Operations, Current Version
(p) NGA MA Standard Operating Procedures, Current Version

ENCLOSURE 2

RESPONSIBILITIES

1. Chief Information Officer (CIO) and Director, IT Services (CIO-T).

a. Carry out the responsibilities in accordance with References (a) through (p).

b. Ensure the reporting of malicious code activity, network compromises and penetration (real or suspected), and other non-authorized network activities in accordance with (IAW) Reference (c).

c. Maintain the external webmail services whitelist and take immediate actions, as required, to safeguard missions (e.g., limiting access to external webmail services to preserve operations security or to preserve bandwidth).

d. Ensure additions to the external webmail services whitelist are approved or denied, based on specific security criteria and thresholds determined by the Authorizing Official (AO) and IAW the risk assessment methodology outlined in Reference (i).

e. Modify the rules, filters, or other measures used to protect NGA's connectivity with the Internet while providing access for NGA personal to approved external webmail services and IbC resources IAW Reference (j).

f. Support investigations of waste, fraud, abuse, and misuse of NGA communications and network resources.

2. Director, Security and Installation Operations (D/SI).

a. Oversee information security practices within the Agency, including the placement of sensitive information on appropriate systems.

b. Ensure all NGA personnel are kept aware of current threats and targets associated with external webmail within DoD and NGA though regular announcements and training.

c. Monitor Internet usage at all NGA facilities and refer all cases of abuse to the Office of the Inspector General.

d. Search and review holdings of Internet data in response to requests from investigators for information related to external or investigative inquiries about Internet abuse.

e. Support investigations of waste, fraud, abuse, and misuse of NGA communications and network resources.

3. Office of General Counsel (OGC). Review the collection and use of information from the Internet and advise personnel on intellectual property, acquisition and intelligence oversight governance. OGC reviews investigations involving possible criminal misuse of Government resources and coordinates investigation and prosecution of computer misconduct.

4. The Office of Inspector General (OIG). Investigate reports of waste, fraud, abuse, and misuse of NGA network resources. In ongoing cases where OGC has initiated contact, OIG coordinates ongoing investigations directly with DoD law enforcement agencies.

5. The Director, Human Development (HD). Support Agency training courses for mission related use of Internet activity.

6. The Office of Contract Services (OCS). Develop and implement the agency procurement policy and ensure effective purchasing practices throughout NGA. OCS is responsible for managing the Agency's DoD Government Purchase Card program and delegate's authority to the purchase card holders to make Internet based purchases. OCS maintains NGA's Blocked Merchant Category List; these merchants are accessible via the Internet.

7. Supervisors and Managers.

a. Ensure that all assigned employees understand the proper use of network resources, including limits (official and unofficial) on Internet access and the use of MA Internet access for those with accounts.

b. Upon OGC approval, support D/SI in response to requests from investigators for information related to external or investigative inquiries concerning external webmail misuse.

c. Approve direct report requests for a MA program level account. Brief the employee and other personnel on the proper uses of the account, and monitor their Internet usage to ensure that abuses of the system do not occur.

d. Document and report instances of suspected abuse.

e. Administer discipline when required.

8. All Personnel (Government and Contractor).

a. Treat all communications over the Internet as unsecure and when authorized for unofficial use, IAW the procedures in this instruction.

b. System administrators or any other privileged users, will not access the Internet while logged in under their elevated privileged accounts, nor will these accounts be used with any Internet sources such as email. All personnel must use their non-privileged user account to access the Internet.

c. May request to add external webmail services to the approved external webmail services whitelist.

d. Immediately report unusual network activity (undue or suspicious activity related to Internet accounts, external email, Internet use, or activities including viruses or malicious code) to the Cyber Security Operations Center.

e. Release to the public only information (products, documents, or data sets) that have been authorized for public release as specified in Reference (n).

f. Refer all requests to OCC from the general public for sensitive or specific NGA, Government, and/or other related information not otherwise publicly available or that may be determined to be released to the public consistent with Reference (n).

g. Consult with OGC regarding any Internet activity that raises legal, ethical, or standards of conduct concerns. Respect the legal protections provided by copyright, license, and authorship of messages, programs, and data on the Internet.

h. Ensure individual accountability and protect network access by not revealing passwords and by not sharing their Internet access accounts.

i. Consistent with Reference (l), comply with Intelligence Oversight, Operational Security, and intellectual property laws and regulations.

j. Refer any concerns dealing with fraud, waste, and abuse of NGA's network resources to the OIG.

k. Adhere to the requirements and conditions for MA account access IAW References (o) and (p). Failure to comply with the conditions set forth in Reference (o) and (p) may lead to administrative disciplinary action.

ENCLOSURE 3

PROCEDURES

1. Internet Usage Overview. NGA employees are provided access to network resources, including the Internet, to conduct official NGA business. Access to the Internet is for the purpose of acquiring information related to assigned duties and responsibilities. Prohibited, or misuse of Internet privileges, is considered misconduct and is subject to administrative disciplinary actions.

a. Official Use and Authorized Purposes of Internet resources.

(1) All personnel may use the Internet for official use. Official use is serving a legitimate NGA interest, such as enhancing professional skills and improving morale when serving an extended period away from home.

(2) Using the Internet for authorized purposes must not adversely affect the performance of official duties, should be of reasonable duration and frequency, and done during the employees break time or lunch period when possible unless otherwise authorized. Examples include; checking in with spouse or children, scheduling doctors, home or auto repair appointments, or performing brief Internet searches.

(3) Use of a NGA email address for other than official duties is unauthorized.

(4) Participating in an Internet blog or discussion as part of an NGA funded educational course or program is permitted when: the subject is not mission related; where NGA's interest in the subject is not considered sensitive or might reveal classified topics of interest; and where the employee does not create the impression that the employee is a spokesperson for NGA. The employee will use the .mil address if participation requires an email address and should disclose their association with NGA if required by terms of the Internet site.

(5) Any activities that could collect personably identifiable information requires approval by OGC prior to operational deployment.

(6) Employees participating in interagency programs where laptops or other collection platforms are used to collect from the Internet may be subject to additional rules and guidelines.

b. Personal Use and Access to Internet-based Resources.

(1) Consistent with Reference (m), employees are authorized limited personal use of network resources and use of an NGA .mil email address for electronic communications. Personal use of official network resources can serve a legitimate

public interest, such as keeping employees at their duty stations rather than requiring the use of commercial systems, improving moral of employees stationed for extended periods away from home, or enhancing professional skills. Personal use of Internet resources should not adversely affect the performance of official duties, should be of reasonable duration and frequency and whenever possible, made during the employees break time such as after duty hours or lunch periods.

(2) Use of an NGA email address account for a communication not related to official duties should be minimized. Reasonable personal use of an NGA email address includes purposes such as: communications with family members, schools, day care, or similar entities. Employees should exercise caution when using an email address as a personal or functional identifier on a website or as method to receive mass or customer communications such as automated news alerts.

c. Prohibited uses of NGA sponsored Internet accounts.

(1) Accessing pornographic sites or downloading images from such sites using NGA sponsored accounts or computer equipment.

(2) Requesting, ordering, creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented material or service for personal recreation or entertainment while utilizing NGA sponsored Internet access.

(3) Downloading unapproved software or playing computer games.

(4) Downloading or disseminating inappropriate material such as hate speech, crude jokes, or material that ridicules or disparages others on the basis of race, creed, sex, color, age, religion, disability, national origin, or sexual orientation.

(5) Business uses unrelated to the employee's official role including:

(a) Personal monetary gain (that is, "for profit" or other activities); or in support of a business activity.

(b) Unofficial participation in any non-NGA fund raising activity.

(c) Endorsement of any product or service.

(d) Participation in lobbying activity.

(e) Any prohibited partisan political activity.

(6) Using NGA sponsored networks or accesses for illegal or unethical purposes such as "hacking", spreading viruses, or disrupting networks.

(7) Permitting anyone else to use one's NGA sponsored access.

(8) Using Government systems as a staging ground or platform to gain unauthorized access to other systems.

(9) Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings regardless of the subject matter.

(10) Creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, or any other illegal activities.

(11) Posting NGA information to external newsgroups, bulletin boards, or other public forums without authority as specified in Reference (l). Employees are specifically not authorized to create the impression that a communication was made in one's official capacity as a Federal employee, unless NGA approval is obtained.

(12) Any use that generates unauthorized expenses to the Government.

(13) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information that includes:

(a) Privacy information

(b) Material subject to intellectual property rights

(c) Proprietary data

(d) Export controlled software or data

(14) Manipulating internet default browser proxy settings to circumvent security settings. Alternate proxy settings are solely for MA Internet access or for individuals with mission justification. Authorization to change proxy settings must come from the CIO or the AO.

(15) Forwarding (automatically or manually) sensitive unclassified information by email to a user's home computer or contractor computer system without CIO or AO approval.

d. Accessing the Internet for an official purpose on a non-Government system.

(1) Use of the Internet when access is not dependent upon NGA government provided equipment for an official purpose, such as assigned research related to an official duty, requires supervisor approval. When an employee has approval to utilize the Internet on non-official equipment for official duties, the following types of information should not be utilized as part of approved Internet access:

(a) Information subject to the Privacy Act and belonging to a person other than the person requesting to work on a non-official system.

(b) Information subject to the Procurement Integrity Act.

(c) Proprietary information unless written approval is received from the owner of the information or from OGC.

(d) Information needed for GEOINT analytic products or research and, where NGA's interest is sensitive or might reveal classified topics of interest to NGA.

GLOSSARY

DEFINITIONS

Authorizing Official	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organization operations (including mission, functions, image, or reputation), organizational assets, individuals other organizations, and the Nation.
Data Transfer Officer	Individual appointed to securely perform authorized data transfers to and from NGA information systems.
GEOINT	The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.
Internet-based Capabilities	All publicly accessible information capabilities and application across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet based capabilities include collaborative tools such as SNS, social media, user-generated content, social software, email, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).
Limited Personal Use	Limited individual communication or activity that is not conducted as an assigned NGA employee.
Managed Attribution	The process of applying obfuscation at various stages within the Cyber Security environment.
Public Release	Information that has been cleared and authorized for general public consumption by the Office of General Council or Office of International Affairs.
Webmail Services Whitelist	Compiled list of webmail addresses that NGA employees are authorized to access from NGA provided information systems.

NI 8470.3~~R8~~ Approved: 9 January 2006
Subgroup: Communications and Electronics *Administrative Update 13 November 2015*

NGA Instruction for Use of Electronic Mail and Other Electronic Communications

1. References.

a. Primary. NGA ~~PD~~ 8000~~R3~~, ~~Policy Directive for~~ Information Management and the Chief Information Officer, ~~24 November 2003~~ *12 June 2013*.

b. Secondary.

(1) NI 5500.11~~R3~~, ~~NGA Instruction for Standards of Conduct, 5 January 2004~~ *Maintaining the Highest Standards of Ethical Conduct Program, 01 October 2008*.

(2) *NGAI* 5720.1~~R7~~, ~~NGA Instruction for~~ Clearance for Public Release, ~~5 January 2004~~ *12 May 2015*.

2. Purpose. Establish guidelines for the use of electronic mail (e-mail) and other electronic communications including communicating via NGA news groups, public folders, facsimile (fax) machines, or telephone networks. This instruction supersedes NI 8470.3R7, same title, 5 January 2004.

3. Policy.

a. Use of NGA electronic communications systems is a privilege. Misuse of electronic communications systems is a violation of the Standards of Ethical Conduct (DoD 5500.7-R, cited in reference 1.b.(1)) and inconsistent with NGA standards of professionalism and responsible behavior.

b. All electronic communications composed, transmitted, or received on NGA electronic communications systems by any individual are and remain the property of NGA. They are not the private property of any NGA personnel.

c. U.S. Government electronic communications systems are subject to monitoring. Anyone's use of U.S. Government electronic communications systems constitutes his or her consent to be monitored. Unauthorized use may subject the individual to criminal sanctions or other administrative adverse or disciplinary action (such as loss of communications privileges or punishment up to and including removal).

4. Scope and Applicability. This instruction applies to all personnel with access to NGA computer networks. It establishes the guidelines for communicating with electronic mail, fax, telephone messaging, or other forms of electronic communications. Guidelines for the use of the Internet, web pages, and Internet browsers are addressed in other NGA instructions.

5. Definitions.

a. Electronic communications system. A combination of computer hardware and software capable of transmitting, receiving, processing, and storing information in digital form. This term applies to any electronic communications system and includes e-mail, news groups, public folders, fax machines, telephones, and other methods and technologies NGA may establish.

b. Electronic mail (e-mail). Dissemination of messages and documents from a sender to recipients using mail messaging capabilities on electronic communications systems.

6. Responsibilities.

a. The ~~Enterprise Operations Directorate~~ *Chief Information Officer-Director, IT Services (CIO-D/T)* is the office of primary responsibility for the implementation of this instruction.

b. The Security and Installation Operations Directorate (SI), Security Office (SIS), Computer Security Division, (SISC), Computer Investigation and Analysis Branch (SISCI) investigates reports and allegations of abuse and misuse of NGA communications resources.

c. The Office of General Counsel (OGC) collects facts, and interprets and determines the applicability of laws, regulations, directives, instructions, memorandums, and guidance documents in support of SISCI investigations into allegations of abuse or misuse of Government computer resources.

d. The Human Development Directorate (HD) supports SISCI during investigations into allegations of abuse or misuse of communications systems and reports to OGC all personnel actions taken based on abuse and misuse of electronic communications systems.

e. The Office of Corporate ~~Relations~~ *Communications*, Corporate Communications Division, Public Affairs Division (*OCRCNP*) administers the public release policy and coordinates the review of all information (printed and electronic) regarding NGA mission and functions and is intended for public release. OCRNP reviews and approves all official and unofficial announcements proposed for posting on the NGA intranet home page.

f. Supervisors routinely monitor computer usage in the work areas for which they are responsible. On request of subordinate personnel, supervisors carefully review and approve proposed global distribution e-mail messages for appropriate content and purpose.

g. Personnel must

(1) Always consider the potential resource impact to NGA electronic systems before sending electronic communications to wide audiences.

(2) Use common sense and good judgment when using NGA electronic communications systems.

7. Procedures.

a. Use of electronic communications systems. In addition to the uses prescribed by the Joint Ethics Regulation (cited in reference 1.b.(1)), employee use of electronic communications must follow the normal courtesies common in official correspondence. Examples of inappropriate uses of NGA electronic communications systems include

- Disparaging or derogatory comments attacking someone's character or integrity, including profanity and other abusive language.
- Venting personal frustrations to a wide audience.
- Discussing or transmitting classified information on systems that are not appropriately secured for such discussions or transmittals.
- Conducting unofficial business on behalf of a commercial enterprise.
- Incurring long-distance or other use charges for unofficial calls or fax transmissions.
- Sending chain letters.
- Espousing one's political or religious beliefs or sentiments.

b. Inappropriate use of NGA e-mail global addresses (such as All NGA Government, All NGA Bethesda, and All NGA St. Louis) constitutes an abuse of the privilege and may result in loss of access to e-mail applications (alternative approaches for personal announcements are listed in paragraph 7.k.). Inappropriate uses include

- Sending unofficial games, catalogs, recipes, stories, or holiday messages.
- Making announcements concerning "lights on," "lost and found," new phone numbers or office locations, unofficial virus alerts, and similar unofficial broadcasts.
- Publicizing unauthorized activities (including those listed in paragraph 7.a.) such as charity solicitations, baby showers, retirements, or farewells.

- Political campaigning or other political activities.

- Personal advertising, soliciting, or selling.

c. Communications system users must give special attention to documents and attachments being transmitted to members of the general public. Information pertaining to the mission and functions of NGA and intended for public release by any means is subject to review by relevant NGA offices. If the information concerns or affects the plans, policies, programs, or operations of DoD, the IC, the U.S. Government in general, or NGA in particular, and it has not been cleared for public release, it must be approved under the formal review process described in *NGAI* 5720.1~~R7~~.

d. Supervisors at pay band NI 4 or higher or military officers at the field-grade level or higher may, on a case-by-case basis, authorize individuals to use NGA e-mail for limited personal communications that are most reasonably made from the office. Limited use of telephones and fax machines for personal uses most reasonably made from the office, such as informing family of longer-than-expected working hours, arranging auto repair or medical appointments, or applying for jobs outside the Agency, are authorized without supervisor intervention. Personal use of electronic communications systems must not adversely affect the performance of official duties by the individual or the individual's organization, result in added costs to the government, or overburden the system.

e. Personnel at NGA sites who are provided electronic communications services by other government Agencies must comply with NGA standards for their use and with all requirements of the individual system on which they are working.

f. Unless a specific exemption is approved, this instruction will be included in the terms of contracts in which contractor personnel are authorized to use NGA systems in contract performance. Contractor personnel should be aware of contract limitations prior to sending messages, including any terms pertaining to inspection, review, and content of messages sent via NGA electronic communications.

g. Inspection of messages. All personnel using faxes and electronic mail must carefully and consistently inspect the content and evaluate the purpose of messages or documents for appropriateness and adherence to NGA policy before faxing, posting, sending, or forwarding.

(1) **Before** sending e-mail messages, check the address box to ensure that only the appropriate audience is addressed.

(2) **Before** sending e-mail messages or faxes to external recipients, carefully review any attachments from within the body of the message for appropriateness, sensitivity, and classification. Do not use the "reply to all" capability unless you have validated that all who would receive the message are authorized to have that information. If the attachment is being forwarded to a member of the general public and contains official information cited in paragraph 7.c., the transmitter must ensure it has been cleared for public release.

(3) **Before** opening attachments to e-mail messages received from external sources, consider your level of trust in the sender's environment.

(4) In e-mail messages addressed external to NGA consider using aliases or developing personal address groups for NGA employees (when appropriate), rather than revealing the individual e-mail addresses of each NGA person.

h. Wide-audience distribution. The use of global addresses (such as All NGA Government, All NGA Bethesda, and All NGA St. Louis) for e-mail is reserved for supervisor-preapproved messages. Some examples of preapproved messages are security alerts from SIS, assignment opportunity notices from HD, and SI Pulse messages. Personnel must obtain prior approval from their supervisor (pay band NI 4 or field-grade officer or above) before transmitting messages to wide audiences using the NGA-wide or NGA-site specific e-mail addresses (for example, All NGA Government, All NGA Bethesda, and All NGA Washington). Supervisors must use prudence when approving electronic mail messages intended for wide audiences. Supervisors should consider requiring their personnel to forward approved global e-mail messages to supervisor's workstation for global transmission. The following questions should be considered before approving broadcast messages:

- Does the sender, approving supervisor, or organization have the responsibility for disseminating the information contained within the message?
- Is the subject matter in support of NGA operations and of interest to wide audiences?
- Is the subject matter within the sender's specific job duties?

i. Information security and remote access. Supervisors and employees must ensure that only NGA-approved access control and encryption mechanisms are used for remote access to NGA electronic communications systems. Authorized remote users must access their Sensitive But Unclassified messages via the approved dial-up connection. Individuals with access to NGA electronic communications

systems open and review any messages or documents they intend to forward to their personal (home) e-mail accounts before sending. Faxes and e-mails should not be sent to numbers or accounts where the possible recipients are not known (such as shared e-mail accounts or fax numbers of commercial fax service providers).

j. Network impacts. Personnel should always consider the impact to network resources that may result from sending attachments to multiple recipients. To minimize the use of attachments, always consider using "cut and paste" to incorporate the information into the message body of an e-mail message or posting documents in folders (directories) accessible to the target audience.

k. Preferred practices. To minimize misuse of electronic communications systems for routine, day-to-day matters, alternative arrangements are available.

(1) Found objects should be turned in to the building security desk and, optionally, may be announced through *OC~~R~~CNP* in the NGA announcements.

(2) Cars with "lights on" and other issues relating to personal vehicles on NGA grounds should be reported to the building security desk. Reports should include the hang-tag number or license plate number of the vehicle.

(3) Unofficial announcements (for example, farewells, thank-yous, and unofficial retirement activities) should be submitted to *OC~~R~~CNP* for inclusion in the NGA announcements.

(4) E-mail should be directed to appropriate interested recipients only. Develop, maintain, and use appropriate group mail lists (user interest groups) as opposed to broadcasting messages to wide audiences. This option is recommended for recurring announcements such as timekeeper updates, excess supply notices, and production system status.

(5) Long-distance telephone and fax activities within the minimal levels allowed in this instruction (paragraph 7.d.) should be charged to a personal billing card, a third party, or the recipient (that is, reverse charges).

(6) Telephone, fax, and e-mail actions beyond the minimal levels allowed in this instruction should be arranged through commercial services (for example, pay telephones, copy providers, and Internet providers) and paid by the individual.

PN 8470.1 Approved: 12 August 2011
Subgroup: Communications and Electronics *Validated Current as of 15 November 2015*

Policy Notice for
External Webmail Access for Personal Use

1. Authorities.

a. NGA ~~P~~D 8000~~R3~~, ~~Policy Directive for~~ Information Management and the Chief Information Officer, ~~24 November 2003~~ *12 June 2013.*

b. CNSSP-22, Information Assurance Risk Management Policy for National Security Systems, February 2009

c. Directive Type Memorandum (DTM) 09-26, Responsible and Effective Use of Internet-based Capabilities, February 22, 2011.

d. NI 5500.11~~R4~~, NGA Instruction for *Maintaining the Highest* Standards of *Ethical* Conduct *Program*, 2 October 2008.

e. NI 8420.3~~R6~~, NGA Instruction for Controlled Interfaces for Systems and Networks, 28 October 2008.

2. Purpose. Provide Agency guidance for the reasonable and responsible personal use of external webmail services on NGA's Sensitive but Unclassified (SBU) network consistent with NI 5500.11R4 (reference 1.d.).

3. Rationale. This notice serves as interim policy pending updates to NGA Instruction 8470.2~~R8~~ "Internet Usage" which will be modified within 365 days of the effective date of this policy notice. This notice supersedes section 7.d.(14) only; the remainder of NI 8470.2~~R8~~ remains in effect.

4. Policy. Consistent with applicable laws and regulations,

a. NGA may provide access to externally based webmail capabilities for personal use on NGA's SBU network.

b. In support of protecting the information and information systems entrusted to NGA, users will exercise good judgment and comply with operational security (OPSEC) when utilizing external webmail access for personal purposes. Use of NGA networks is subject to monitoring at all times.

5. Responsibilities.

a. The ~~Office of the~~ Chief Information Officer-*IT Services (CIO-T)*, Information Security Management Office (*~~O~~CIO-T/CS*) maintains the approved external webmail services whitelist on behalf of the Authorizing Official (AO) and notifies the Controlled Interface Policy Board (CIPB) of additions and/or removals per NI 8420.3~~R6~~ (reference 1.e.). The AO will take immediate and commensurate

actions, as required, to safeguard missions (e.g., limiting access to external webmail services to preserve operations security or to address bandwidth constraints). Additions to the external webmail services whitelist will be approved based on specific security criteria and thresholds determined by the AO and in accordance with the risk assessment methodology outlined in Committee on National Security Systems Policy 22 (CNSSP-22) (reference 2).

b. The ~~Enterprise Directorate, Enterprise Service Operations Office (ES)~~ *CIO-T* modifies the rules, filters, or other methods of NGA's connectivity with the internet to provide access for NGA personnel to approved external webmail services as defined in the external webmail whitelist provided by ~~*O*~~*CIO-T/CS* and in accordance with CIPB procedures in NI 8420.3~~R6~~ (reference 1.e.).

c. The Security and Installation Operations Directorate, Security Office, Computer Investigation and Awareness Division (SISC) ensures all NGA personnel are kept aware of current threats and targets associated with external webmail within DoD and NGA through regular announcements and training.

d. Supervisors and Managers, in support to SISC, review holdings of external webmail related data in response to requests from investigators for information related to external or investigative inquiries about external webmail misuse.

e. NGA personnel:

(1) may request to add external webmail services to the approved external webmail services whitelist. If NGA personnel receive a Denial Notice due to the webmail service being blocked, complete and submit the Cyber Security Change Request (CSCR) form which is available via the link on the Denial Notice.

(2) should not access external personal webmail services when using non-attributable Internet access.

The Hatch Act: Election Campaigns Rules for NGA Employees

Political participation by civilian employees is governed by the Hatch Act (5 U.S.C. 7321-7326). Military personnel refer to Department of Defense (DoD) Directive 1344.10. However, the entire workforce – civilian, military, and contractor – must adhere to restrictions imposed by National Geospatial-Intelligence Agency (NGA) managers for the purpose of maintaining good order and discipline within the workplace. The Intelligence Community (IC), including NGA, has more restrictions than the average Federal employee.

It is a violation of the Hatch Act to engage in "political activity" any time a Federal employee is on duty, in a government facility, or using government equipment. "Political activity" means activity intended to benefit a political party or a partisan political candidate.

NGA Personnel May NOT:

- Display political buttons, posters, or bumper stickers in the workplace. Bumper stickers on personal vehicles parked in NGA (or other Government building) parking lots is permissible.
- Solicit or receive political contributions
- Hand out campaign literature or volunteer to stuff envelopes for a partisan candidate
- Host, sponsor, manage, organize or be featured speaker at a political fundraiser
- Canvas votes for a political candidate, political party or partisan group
- Drive voters to a polling place for a candidate, political party or partisan group
- Serve as delegates, alternates or proxies to political conventions
- Allow the use of their official titles in relation with a political activity

NGA Employees MAY:

- Display political buttons, posters, and signs outside the workplace
- Attend a political rally (not on Government time)
- Vote and sign a political petition
- Contribute financially to a political party or a partisan group or candidate
- Serve as election judges if the law requires non-partisan duties
- Be a candidate for non-partisan office
- Be politically active on an issue or question not identified with a particular political party