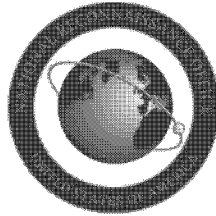


National Reconnaissance Office
Business Function 50, Information Technology,
Information Assurance, and Information Management
**Directive 50-07, Appropriate Use of NRO Information
Technology**



25 SEPTEMBER 2015

TABLE OF CONTENTS

(U) 50-07 CHANGE LOG 3

(U) SECTION I - INTRODUCTION 4

(U) SECTION II - APPLICATION 4

(U) SECTION III - REFERENCES/AUTHORITIES 4

(U) SECTION IV - POLICY 5

(U) SECTION V - ROLES AND RESPONSIBILITIES 8

(U) SECTION VI - DIRECTIVE POINT OF CONTACT 11

(U) APPROVING SIGNATURE 11

(U) APPENDIX A - ACRONYM LIST 12

(U) APPENDIX B - GLOSSARY 13

ND 50-07 Appropriate Use of NRO Information Technology
 FY 2015

(U) 50-07 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks
1.1	June 2014	CIO [redacted]	ALL	Updated references and conducted annual review.
1.2	25 Sep 15	COMM/ [redacted]	ALL	Updated all sections which are incorporated by reference into CIO Note 2015-1, Standard Security Banner for Information Technology Systems, dated 5 May 15. CIO Note 2014-1, dated 21 Nov 14, has been rescinded. Updated Glossary.

(b)(3)

(b)(3)

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, this NRO Directive (ND) defines the scope, authorities, and responsibilities specific to NRO Business Function (NBF) 50, Information Technology, Information Assurance, and Information Management (IT-IA-IM). The ND is coordinated with appropriate stakeholders, and is approved by the NBF owner, with administrative approval of the Director, Office of Policy and Strategy (OP&S). Official record copies are archived by OP&S.

(U) This ND establishes the policy for the appropriate use of NRO Information Technology (IT). It defines the actions users must take to ensure their activities are legal, authorized, ethical, and secure when using NRO-owned or sponsored IT. The NRO has a zero-tolerance policy for misuse or abuse of IT. Access to NRO IT, to include NRO sponsored Internet access, is a granted privilege subject to NRO policies and applicable local, state, and Federal laws.

(U) SECTION II - APPLICATION

(U) All NRO personnel who perform tasks or have duties specific to NBF 50 will comply with this ND and its corresponding instructions. When the work to be performed under an NRO contract must comply with this directive and corresponding instructions, the program office shall list these documents as reference documents in the contract statement of work.

(U) SECTION III - REFERENCES/AUTHORITIES

a. (U) Executive Order 12958, Classified National Security Information, as amended, 25 Mar 03

b. (U) Title 5 United States Code Section (a) 552a, Privacy Act, as amended, 1974

c. (U) Title 17 United States Code Section 106, Copyright Law, as amended, 23 Jul 93

d. (U) Presidential Policy Directive 28, Signals Intelligence Activities, 17 Jan 14

e. (U) Office of Budget and Management M-06-16, Protection of Sensitive Agency Information, 23 Jun 06

f. (U) Intelligence Community Directive 208, Write for Maximum Utility, 17 Dec 08

**ND 50-07 Appropriate Use of NRO Information Technology
FY 2015**

- g. (U) National Reconnaissance Office Business Function 50, Information Technology, Information Assurance, and Information Management, 8 Apr 13
- h. (U) National Reconnaissance Office Business Function 100, Security and Counterintelligence, 3 Apr 12
- i. (U) National Reconnaissance Directive 50-20, Portable Electronic Devices, 24 Feb 14
- j. (U) National Reconnaissance Office Directive 52-05, Assessment, Authorization and Monitoring, 8 Jun 13
- k. (U) National Reconnaissance Office Directive 53-20, Unclassified Management Information Service Account Qualifications and Access Management, 10 Feb 14
- l. (U) National Reconnaissance Office Directive 53-21, Contractor Local Area Network Account Management, 27 Sep 13
- m. (U) National Reconnaissance Office Directive 53-22, National Reconnaissance Office Management Information System Account Qualifications and Access Management, 28 Feb 12
- n. (U) National Reconnaissance Office Directive 53-23, Secret Collateral Management Information System Account Qualifications and Access Management, 13 Mar 13
- o. (U) National Reconnaissance Office Directive 53-24, Non-Associated Services, 17 Oct 13
- p. (U) National Reconnaissance Office Directive 56-02, Information Review and Release, 20 Feb 14
- q. (U) Chief Information Officer Policy Note 2015-01, Standard Security Banner for Information Technology Systems, 5 May 15. NOTE: Replaces Chief Information Officer Policy Note 2014-11, Banners for Information Technology Systems, dated 21 Nov 14, which has been rescinded

(U) SECTION IV - POLICY

(U) Use of the NRO Information Enterprise (NIE), to include NRO sponsored Internet, is covered under the same NRO regulations and procedures that govern computer fraud and misuse. Users must not attempt to gain unauthorized privileges or intentionally attempt to access information that is not required for their official duties.

~~(U//FOUO)~~ All information, including classified information, processed, stored, or disseminated via any United States Government

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

(USG)-authorized information system and access account shall be utilized only for USG-authorized purposes and only by users having a verifiable need-to-know. Contractor employees shall use USG-authorized information systems only for USG-authorized purposes within the scope of their NRO contracts. USG-authorized information systems include:

- a. The computer utilized by the user;
- b. The software installed on such computer;
- c. The computer network associated with such computer;
- d. All computers connected to such network; and
- e. All devices and storage media attached to such network or to a computer on such network.

(U) All USG-authorized systems are subject to monitoring, interception, and search of the user's communications and activity for all lawful purposes, including but not limited to, administration, maintenance, management, testing, security, counterintelligence, law enforcement, or any other official purpose. Monitoring, interception, and search may include, but not be limited to, network analysis, automated intrusion, misuse detection systems, access, audits, logging, keystroke monitoring, and full-text review of files, electronic mail messages, and instant messages for all lawful purposes, to include ensuring the availability, integrity, and confidentiality of sensitive USG information.

(U) Limited incidental personal use of the Internet is acceptable; however, the user shall charge time spent as personal time. Limited incidental personal use is permitted if it does not:

- a. (U) Jeopardize an NRO employee or contractor's association status;
- b. (U) Include research that may reveal sensitive geographic locations or government/military affiliations;
- c. (U) Adversely affect the ability of the employee to fulfill their official duties;
- d. (U) Disrupt NRO activities;
- e. (U) Result in inaccurate time charging;
- f. (U) Incur a measurable cost to the NRO; or

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

g. (U) Involve illegal, obscene, defamatory, prohibited fundraising, or commercial activities.

(U) Transmission of classified material over unclassified systems or systems of lower classifications is prohibited.

(U) Transmission of trademarked or copyrighted information is prohibited without appropriate intellectual property rights or the express written approval from the Office of General Counsel.

(U) Unclassified For Official Use Only (FOUO) information is permitted on Government sponsored networks that use the Internet, only if the network has been approved for FOUO information. Users should verify this with their Information System Security Manager (ISSM), Information System Security Officer (ISSO), or Program Security Officer (PSO). FOUO data must not be posted on any public site.

(U) All authorized USG activities requiring electronic mail shall be conducted using NRO-issued electronic mail accounts. Unapproved accounts, such as web-based commercial electronic mail accounts, shall not be used for official USG business unless specifically authorized by the Designated Authorizing Official. Internet service provider or web-based e-mail systems will be approved only when communication is mission essential and USG owned e-mail systems are not available.

(U//~~FOUO~~) One-way electronic transmission from unclassified to classified systems is permissible if this process is performed in accordance with approved file transfer processes/procedures. Electronic transmission from classified to unclassified systems is permitted only if the information is unclassified, does not violate the security posture of the destination domain and approval is coordinated via NRO Form 5-23, File Transfer Authorization Request, or comparable form at non-headquarters sites. Users needing assistance should seek guidance from their ISSM or ISSO.

(U) Any information about, or affecting the plans, policies, programs, or operations of the NRO or USG, that is proposed for public release over the Internet shall be reviewed and approved in accordance with ND 56-02, Information Review and Release, prior to release, publication, posting to a web site, or transmission.

(U) USG-purchased or contractor-provided hardware and software may not be connected to the NIE without the approval of the Chief Information Officer and successful completion of the NRO Assessment and Authorization Process in accordance with ND 52-05, Assessment, Authorization and Monitoring or other applicable processes.

(U) Personally-owned hardware and software shall not be connected to the NIE.

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

(U) Contractor personnel have the legal obligation and ethical duty to safeguard sensitive USG information. Subject to all other provisions of this directive on access and use, including limited incidental personal use of the USG-authorized information system, contractors shall use the information accessible through the NIE, and any related communications, only to fulfill the requirements and duties specified in their USG contracts or to accomplish USG-authorized activities, and shall access only that information for which they have a verifiable need-to-know. Use for marketing, gaining advantage in a competitive acquisition over other contractors, or other commercial activities is prohibited with the exception of actions taken in anticipation of, or in response to, official USG-authorized business.

(U) Violators of this policy will face disciplinary actions that may include, but not be limited to, verbal or written reprimands, loss of account privileges, loss of access, termination of employment, or other administrative disciplinary enforcement, civil liability, or criminal prosecution according to applicable laws, NRO policies, and security requirements.

(U) An NRO-authorized log-on banner (reference q), summarizing this policy, shall be displayed on all information systems under an NRO Assessment and Authorization authority, prior to user log-on to obtain user consent to the provisions of such policy. Additional banners notifying the user of privacy or protection of personal data requirements may be used prior to log-on in accordance with Presidential Policy Directive 28, Signals Intelligence Activities (reference d).

(U) SECTION V - ROLES AND RESPONSIBILITIES

(U) Users shall:

- a. (U) Use the NIE for official USG business;
- b. (U) Not use the NIE to conduct personal or corporate business development;
- c. (U) Ensure that personal use of social networking sites such as Facebook, Twitter, and LinkedIn is on a limited basis;
- d. (U) Be subject to monitoring, interception, and search of the user's communications and activities, including incidental personal use;
- e. (U) Recognize that authorized officials may examine, record, copy, and appropriately disclose any information discovered in the course of such lawful monitoring, interception and search activities. System officials may provide evidence of intrusion,

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

misuse, misconduct, criminal activity, or other malicious activities to the appropriate law enforcement or other authorities for appropriate action, which may include, but not be limited to, criminal investigation and administrative disciplinary enforcement;

f. (U) Have no expectation of privacy regarding all communications, data transmissions, stored data, or activities conducted on the NIE. However, USG monitoring, interception, and search of the user's communications and activities on the system does not waive or alter legal protections or exemptions under the Privacy Act, Freedom of Information Act, legally privileged communications or work products associated with attorneys, medical professionals or clergy, and any legal rights in intellectual property or proprietary information;

g. (U) Only use their authorized account to access information when using their logon identification and password. Users are responsible for all activity that takes place on their user account;

h. (U) Use strong, unique, and separate passwords for each NIE system. Sharing user login credentials is prohibited unless a justification demonstrating a mission requirement is approved by the Program Manager and PSO;

i. (U) Adhere to NRO and local site configuration management requirements and understand they may not reconfigure any system or make any unauthorized changes to system hardware or software;

j. (U) Adhere to all security practices and guidelines for safeguarding classified and sensitive information;

k. (U) Report all information assurance related security incidents, potential data spills, and suspicious or abnormal system activities to the PSO, ISSM, or ISSO immediately;

l. (U) Comply with the requirements and prohibitions that govern the collection, retention, and dissemination of information regarding United States (U.S.) persons;

m. (U) Recognize that unauthorized collection, transmission, or use of sensitive USG information can result in severe consequences for all parties involved, including criminal punishment, civil liability, administrative disciplinary enforcement, and revocation of access;

n. (U//~~FOUO~~) Protect associations as required. Unclassified NRO information, if when combined with other unclassified

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

data could reveal sensitive information or classified associations, is prohibited from being transmitted over the Internet; and

o. (U) Adhere to the following principles when using collaborative web-based pages within the Intelligence Community (IC):

1. (U) Add value;
2. (U) Be constructive;
3. (U) Know the user's audience and exercise due care when posting information with the understanding that the information may be reposted on other networks without permission for a wider audience;
4. (U) Take ownership, be responsible for content, and understand that users may not post anonymously on IC Collaboration web sites;
5. (U) Apply the standards established in IC Directive 208, Writing for Maximum Utility and Least Sensitivity (reference f);
6. (U) Inform managers regarding the user's web-based collaborative projects; and
7. (U) Classify properly and follow requirements for pre-publication review in accordance with NBF 50.

p. (U) Complete all NRO mandatory annual training;

q. (U) Read, complete, and abide by all applicable user acknowledgement briefings for NRO sponsored information systems; and

r. (U) Be cognizant of current phishing and other scam trends and avoid them while using the NIE.

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

(U) SECTION VI - DIRECTIVE POINT OF CONTACT

(U) Director, IT Policy and Governance Staff, Communications
Systems Directorate, secure [] and unsecure []

(b)(3)

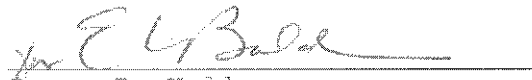
(U) APPROVING SIGNATURE

(U) As the NBF owner for IT-IA-IM, I confirm that this document
provides a complete representation of ND 50-07, Appropriate Use of NRO
Information Technology, and the document has been coordinated with
stakeholders in this process.



Terry S. Duncan
IT-IA-IM NBF Owner

23 Sep 15
Date



Damon R. Wells
Director, Office of Policy
and Strategy

25 Sep 15
Date

~~UNCLASSIFIED//FOUO~~

ND 50-07 Appropriate Use of NRO Information Technology
 FY 2015

(U) APPENDIX A - ACRONYM LIST

Acronym	Term
BIT	Business Information Technology
EIT	Enterprise Information Technology
FOUO	For Official Use Only
IA	Information Assurance
IC	Intelligence Community
IM	Information Management
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
MIT	Mission Information Technology
NBF	National Reconnaissance Office Business Function
ND	National Reconnaissance Office Directive
NIE	National Reconnaissance Office Information Enterprise
NRO	National Reconnaissance Office
OP&S	Office of Policy and Strategy
PII	Personally Identifiable Information
PSO	Program Security Officer
U.S.	United States
USG	United States Government

Table is UNCLASSIFIED

~~UNCLASSIFIED//FOUO~~

ND 50-07 Appropriate Use of NRO Information Technology
 FY 2015

(U) APPENDIX B - GLOSSARY

Term	Definition
(U) Abnormal System Activities	(U) Activities that include changes in program length, changes in date or time stamp, longer program load times or slower system operation, disappearing programs, unexplained disk or drive activities or reduction in memory or disk space, unusual error messages, failed program execution or unexpected reboots, and unusual screen activity or the appearance of files with unusual names.
(U) Association Status	(U// FOUO) Association Status: A mechanism whereby the affiliation of a person, organization, installation, facility, or activity to USG intelligence agencies, organizations, or activities, or in some cases even generically to the U.S. Government itself, is disguised and protected from unauthorized disclosure. Usually provided when that intelligence or governmental affiliation is classified in the interests of national security pursuant to relevant statutes and Executive Orders, and when disclosure of such affiliation reasonably could be expected to cause harm to national security.
(U) Business Information Technology	<p>(U) IT activities associated with the development and maintenance of software and hardware to support business functions to include, but not limited to, human capital, core financials, acquisition, procurement, logistics, grants, asset management, payroll, budget formulation and execution, performance management, travel, time and attendance, cost accounting, project accounting, earned value management, personnel management applications, and elements of security systems that track personnel.</p> <p>(U) Business Information Technology (BIT) also includes all supporting feeder systems that support the Business Management operations of an organization or agency. BIT applications and services shall be available to business systems users via Enterprise Information Technology (EIT) networks and workstations.</p>

ND 50-07 Appropriate Use of NRO Information Technology
 FY 2015

Term	Definition
(U) Enterprise Information Technology	(U) Encompasses IT activities associated with the Agency's infrastructure, such as desktops, local area networks, wide area networks, processors, software, security, operations, help desks, applications, support services, and resources associated with the IT. This category identifies IT elements and applications available to all users of the enterprise (e.g., e-mail). Information assurance capabilities are to be included in this category. Also included in the EIT category are completely installed computer systems and their peripheral components.
(U) Information Assurance	(U) Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
(U) Information Management	(U) Any activity involving: 1) The planning, budgeting, manipulating, and controlling of information throughout its lifecycle, including collection and dissemination, privacy and disclosure, review and release, and records management. 2) The management of data, in all forms, that provides for the proper privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies, to include the disposition of agency records in compliance with all legal, regulatory, and statutory responsibilities.
(U) Information System	(U) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
(U) Information Technology	(U) Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of the preceding sentence, equipment is used directly or is used by a contractor under a contract which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It is further delineated by BIT, EIT, and Mission Information Technology (MIT).

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

Term	Definition
(U) Limited Incidental Personal Use	(U) Brief time taken during the day for personal scheduling, Internet browsing, purchases, family activities, preparation of résumés or school papers, sending e-mail, or other personal matters.
(U) Mission Information Technology	(U) IT activities associated with collection, analysis, and production systems, and information sharing/collaboration tools, applications, and software, with the exception of office automation systems. These systems can exist at the point where information is initially processed or at the point where analysts turn collected information into intelligence and knowledge. MIT also includes special purpose software and IT elements used among small, unique user populations.
(U) National Reconnaissance Office Information Technology Enterprise	(U) Collection of all NRO-owned, and NRO-sponsored information, IT, or information systems required to perform the NRO mission, including mission, business and enterprise IT.

ND 50-07 Appropriate Use of NRO Information Technology
 FY 2015

Term	Definition
(U) Personally Identifiable Information	<p>(U) Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, either alone or when combined with other personal or identifying information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.</p> <p>(U) The definition of Personally Identifiable Information (PII) is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available in any medium and from any source that, when combined with other available information, could be used to identify an individual.</p> <p>(U) Some examples of PII include name, photographic identifiers, distinguishing features, date of birth, email address, mailing address, geographic location data, vehicle identifiers including license plates, unique names, certificate, identification numbers, activities information (e.g., foreign activities and/or interests), government information (e.g., citizenship or immigration status, association with items of interest), telephone numbers and/or other specific reference numbers and/or any information that can identify an individual.</p>
(U) Phishing	<p>(U) A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.</p>
(U) Security Incident	<p>(U) An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.</p>

ND 50-07 Appropriate Use of NRO Information Technology
FY 2015

Term	Definition
(U) Social Networking Sites	(U) Web-based sites designed for creating online environments for individuals and organizations to share information. Most often, individual users are encouraged to create profiles containing various details about themselves. Users can often upload pictures of themselves to their profiles, post blog entries for others to read, search for other users with similar interests, and compile and share lists of contacts.
(U) United States Person	(U) Federal law and executive order define a U.S. Person as: a citizen of the U.S.; an alien lawfully admitted for permanent residence; an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence; and a corporation that is incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments.

Table is UNCLASSIFIED//~~FOUO~~