(U) National Reconnaissance Office (NRO)

(U) Enterprise Operations Security (OPSEC) Plan

01 June 2011

Reviewed: 2 Jun 14

Robert Harney
Director, Office of Security & Counterintelligence

(U) TABLE OF CONTENTS

(U) Record of Changes:

Change Number / Description	Date of Change	Entered By
Annual Review Performed - No Changes	4 Jun 12	
Annual Review Performed - No Changes	17 Jun 13	
Annual Review Performed - No Changes	2 Jun 14	

(b)(3)

1. (U) GENERAL INFORMATION

1.1. (U) Purpose

1.1.1 (U) Operations Security (OPSEC) is a mandated program designed to safeguard critical information (CI), actions related to operations, and other activities which, if exploited by an adversary, could jeopardize operations and lives. This is accomplished by identifying vulnerabilities that could be exploited by intelligence analysis, and eliminating or reducing the risk created by these vulnerabilities to an acceptable level. The purpose of this plan is to establish basic and consistent OPSEC measures, definitions, procedures and enable awareness of issues within the National Reconnaissance Office (NRO). It is to protect information generally available to the public as well as certain detectable activities that reveal the existence of, and sometimes details about, classified or sensitive information. Such indicators may assist those seeking to neutralize or exploit U.S. Government or U.S. Government Contractors' actions in the area of national security. Application of the OPSEC process in the daily activities of all NRO personnel as well as formally in Program Protection planning, promotes operational effectiveness by helping prevent inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

1.1.2 (U) The OPSEC principles contained in this document are basic principles that can be modified for NRO Government facilities, as well as across the entire NRO Industrial base. OPSEC must evolve with each program or activity as Critical Information Lists (CIL), threats and vulnerabilities continue to change throughout program and operational lifecycles. Critical Information (CI) is information, generally unclassified in nature that alone or in compilation can be revealing of classified or sensitive activities. CI differs from Critical Program Information (CPI) which describes the most sensitive information related to a specific NRO program. CPI typically consists of the most highly classified program operational details, system capabilities, cutting edge technologies, and system vulnerabilities and survivability. OPSEC is intended to protect unclassified CI while complimenting Program Protection activities that protect CPI.

1.1.3 (U) It is incumbent on all program personnel, not just security and counterintelligence, to be responsible for, and vigilant about OPSEC

indicators. If you have OPSEC questions or concerns at your facility contact your Program Security Officer (PSO) for further guidance.

1.2. (U) Objective

1.2.1 (U) OPSEC assists the NRO in planning for the protection of NRO systems, data, capabilities, procedures, and assets, as well as personnel, that are essential to the successful achievement of all NRO, Intelligence Community (IC), and Department of Defense (DoD) related missions and responsibilities.

2. (U) OPSEC FIVE-STEP PROCESS

1. Identification of critical information;
2. Analysis of threats;
3. Analysis of vulnerabilities;
4. Assessment of risks; and
5. Application of appropriate countermeasures.

2.1. (U) Identification of Critical Information

2.1.1 (U) Critical information is information about NRO activities, intentions, capabilities or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or complicate mission accomplishment, reduce mission effectiveness, assist our adversary in developing countermeasures or cause loss of lives or damage to friendly resources. Critical information usually involves key elements of information as identified by the NRO and our mission partners (that may be classified or sensitive) concerning activities or intentions that might significantly degrade mission effectiveness if revealed to an adversary. Critical information may also be derived from seemingly unrelated elements of information, usually unclassified in nature, that can in aggregate, reveal technologies, capabilities, vulnerabilities, and operations.

2.2. (U) Analysis of Threats

2.2.1 (U) Access to current threat information is critical to developing appropriate countermeasures. Threat analysis can identify adversaries, their capabilities, and intentions to collect, analyze, and use critical information. Threat information is available to all NRO personnel via [redacted] and threat analysis assistance is provided by OS&CI Program Secuirty Officers (PSO), Counterintelligence Support Officers (CSO), and [redacted] Analysts. In addition, OS&CI [redacted] produces tailored program threat assessments, company assessments, site (b)(3) (b)(3)

assessments, local area threat assessments, foreign intelligence threat overviews (by country), tailored Counterintelligence awareness briefings, Counterintelligence Support Plans, pre-travel/post-travel briefings, and tailored defensive counterintelligence briefings. These products, as incorporated into the overall Program Protection process can contribute to OPSEC awareness and the protection of Critical Information. The following are some general examples of threats an adversary can pose:

1. HUMINT Threat: Human intelligence describes activities to obtain both classified and unclassified information through the use of human agents. Endeavors of human agents (both overt and covert) pose a substantial threat if countermeasures to neutralize or minimize their activities are not employed.

    a. Overt – Open Source Intelligence (OSINT) Information and Literature: Significant quantities of unclassified documents (both formal as well as in-house distribution and coordination items) offer a lucrative target to an adversary. OSINT is available from the news media, public affairs announcements, press leaks, resumes, public hearings, job postings, and contracts or contract related material, the internet and personal observation. Request for documents under the Freedom of Information Act (FOIA) and mining of information from official web sites must be anticipated.

    b. Visitors – Visitors to facilities include, but are not limited to government personnel, subcontractors, vendors, suppliers, contractors, and service personnel (repairmen, telephone, janitorial, etc.) who may obtain information of interest to an Intelligence Service. The greatest danger to NRO programs is the possible visual and aural disclosure of information that could inadvertently occur during visits by uncleared personnel, as well as cleared personnel without a valid Need-to-Know.

    c. Covert – Illegal Entry/Coercion/Collusion (Espionage). This kind of intelligence gathering includes all clandestine and illegal activities and operations of Intelligence Services.

2. SIGINT Threat: SIGINT describes the capability to obtain classified and certain unclassified information by monitoring communication systems, or by analyzing electromagnetic radiation/emanations from various types of equipment. Most activities and organizations are highly susceptible to the SIGINT threat. SIGINT is derived from signal interception and includes all Communications Intelligence (COMINT),

Electronics Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT). Prime SIGINT sources can include but are not limited to clear voice (unencrypted) telephones, fax machines, cell phones, portable electronics and computer-to-computer data connections. Any machine processing data electronically is vulnerable to clandestine, remote, or electronic interception. Telephone conversations are especially vulnerable because most are relayed, at some point in transmission, via microwave signals or via satellite, both of which are easily monitored. The use of talk-around is not effective as a means to protect critical or sensitive information during telephone conversations.

3. IMINT Threat: IMINT describes the capability to derive information from imagery developed over the full range of the electromagnetic spectrum. Applications of IMINT include hand-held photography, satellites, scheduled commercial aircraft and private aircraft overflights that employ advanced photographic techniques.

2.3. (U) Analysis of Vulnerability

2.3.1 (U) Vulnerabilities exist when adversaries are capable of collecting information, correctly analyzing it, and using it to their advantage. Some practices that may be exploited are:

1. The use of non-secure telephones/fax machines/PDAs to discuss or pass sensitive program information (remember compilation of data);
2. Practices revealing the nature of the association between the NRO/Industry and its customers, prime contractors and subcontractors, critical supply-chain interfaces, etc; and
3. Observable activities such as:
   a. After hours recall to program areas;
   b. Support provided to or received from specific Government agencies;
   c. Task orders preparations to include personnel assignments, etc;
   d. Increase in clerical activity, such as travel arrangements, job interviews, etc;
   e. Increased activity between company contracts and Government personnel;
   f. Logos and memorabilia;
   g. Internal and public job or position posting details; and
   h. Travel patterns by specific U.S. Government or contractor personnel.

2.4. (U) Assessment of Risks

2.4.1 (U) Risk assessment is a structured process that evaluates the risks of critical information loss or compromise, based on an analysis of threats to, and vulnerabilities of the program(s). Risk management considers the risk assessment, along with the availability, efficiency, and costs of countermeasures, as an underlying basis for making appropriate OPSEC decisions. The selection of OPSEC measures must be based on their ability

to preserve our effectiveness, while limiting the exploitation of critical information to the maximum extent possible.

2.5. (U) Application of Appropriate Countermeasures

2.5.1 (U) OPSEC measures work to reduce or eliminate vulnerabilities that point to or possibly divulge critical information. They help protect critical information by controlling the raw data, observables and the OPSEC indicators used by adversaries to identify and exploit NRO programs and capabilities. The most desirable OPSEC measures are those that combine the highest possible protection with the least impact on operational effectiveness, as well as minimal impact to program cost, schedule, and mission capability.

3. (U//~~FOUO~~) NRO CRITICAL INFORMATION LIST (CIL)

(b)(3)

* (U) The above list is not all encompassing. Additional program specific OPSEC concerns and critical information items must be documented in Major Systems Acquisition (MSA) Program Protection Plans (PPP).

4. (U) OPSEC CONSIDERATIONS

4.1. (U) Use of non-secure phones

4.1.1 (U) Change has taken place with regard to the non-secure (black) phone lines used by Westfields personnel. In the past, when placing commercial phone calls, non-secure telephone numbers within the Westfields facility were blocked from display on the receiving end. In order to correct recurring connectivity issues and ensure the level of service the population is accustomed to, the block has been removed.

4.1.2 (U) Non-secure (black line) telephone numbers within the NRO Westfields facility were previously blocked from display on the receiving end. Now when placing phone calls from black phones within the NRO HQ facility, the originating phone number will display as [redacted] (last four digits do not reflect the caller's extension) on calls placed to phones equipped with caller ID. The [redacted] and not associated solely with the NRO facility or NRO employees. However, the history of [redacted] as a prefix predominately used by the NRO HQ is apt to suggest an NRO affiliation. (b)(3) (b)(3) (b)(3)

4.1.3 (U) As a mitigation, NRO personnel must, whenever possible, use the secure phone line when conducting NRO business with individuals in classified or sensitive environments. Never discuss or "talk around" classified information on the unsecure phone line or hold classified conversations in an area where anyone is using an unsecure line. In addition, if anyone in your immediate area is using a secure line; refrain from making or receiving any phone calls on the unsecure line. It is best practice when in a SCIF to always inform others in the immediate area when using an unsecure line. This will help to ensure no classified discussions are inadvertently disclosed over the phone.

4.2. (U) Avoiding "Talking Around" Classified Information

4.2.1 (U) NEVER talk around classified information/material in uncontrolled circumstances whether it is in person, on the black phone or on unsecure electronic devices. If you believe the conversation may lead to a classified discussion, it must be held in an accredited SCIF. Individuals are reminded of compilation issues when dealing with unclassified information/data. To ensure proper OPSEC at the NRO, classified discussions are not permitted in the following locations:

1. Cafeteria;
2. Lobbies;
3. Parking Garages;
4. Hallways;
5. Bathrooms;
6. Smoking areas;
7. Fitness center;
8. Personal or Government vehicles; and/or
9. Any other public area.

4.2.2 (U) Use an accredited SCIF suite or conference room for classified or sensitive discussions to avoid the risk of an uncleared visitor or someone without the Need-to-Know overhearing the conversation.

4.3. (U) Badges

4.3.1 (U) Holders of IC badges must take the following OPSEC precautions: when leaving work, badges must be removed and secured so they cannot be easily seen. If the badge is not removed or is easily seen, an adversary can ascertain that you are a member of the IC; making you and your family a potential target.

1. Do not wear your badge outside of controlled areas, which includes: public transportation, at a restaurant, in the grocery store, picking your kids up at school, or anywhere people you don't know could see your badge;
2. Do not leave your badge in your car overnight or leave it in view while unattended;
3. Do not use your IC badge at a non-IC facility;
4. Do not use your IC badge as proof of a government ID when checking into a hotel; and
5. While on travel, use your Common Access Card (CAC) for official use only.

4.4. (U) Introduction of Cell Phones, Communication Devices, etc.

4.4.1 (U) Use of various electronic devices in NRO buildings or accredited SCIFs may inadvertently compromise the confidentiality, integrity or availability of NRO information. For this reason, NRO policies restrict or prohibit some of the technologies associated with these devices.

4.5. (U) Use of Computer/Internet/Laptops

4.5.1 (U) OPSEC precautions must be taken when traveling with an official government or contractor-provided program laptop. NRO Information System Security Officers (ISSO) manage all government issued laptops and can assist in ensuring the following:

1. Ensure all unclassified laptops have the Basic Input/Output System (BIOS) locked down with administrative password to prevent unauthorized system access. The function of the BIOS is used to configure the basic operation of a computer. It is the first program to run when the computer boots up. It loads the operating system, while setting up all other devices that are found on your computer;
2. All Universal Serial Bus (USB) ports, unless specifically approved for use, must remain disabled to prevent unauthorized system port access;
3. A strong password, in compliance with security requirements, must be established prior to departure;
4. Establish timed screen locks of 15 minutes or less on all laptops;
5. The laptop must have the latest antivirus updates, Information Assurance Vulnerability Alert (IAVA) patches, and enabled data-at-rest encryption;
6. All other mitigations, such as metal tape over infrared devices and/or microphone disabling plug insertion, shall remain in place;

7. System auto launch features must be disabled to prevent media execution upon insertion into a system;
8. Laptops, if specifically approved for Internet connection, must have the Internet firewall enabled; and/or
9. All accounts msut be locked, with screen saver enabled and/or log off if left unattended.

4.5.2 (U) There are other devices such as Personal Digital Assistants (PDA), Smart Phones, etc. used for travel that also have OPSEC indicators and concerns such as unsecure wireless, software applications and downloads.

4.5.3 (U) Understand that adversaries including foreign intelligence groups can gain access to any of the following on your computer and/or laptop without your knowledge:

1. E-mail logs;
2. Software Registration Records;
3. File Structure;
4. Network Log-ons;
5. Cache;
6. Names, Addresses, Identity Numbers;
7. Credit Card Numbers, Bank Accounts; and
8. Phone Numbers.

4.5.4 (U) Steps you can use to protect your personal information and promote proper internet safety:

1. Turn off internet cookies;
2. Update anti-virus software with new definitions;
3. Protect your passwords;
4. Create accounts with strong passwords (i.e. uppercase, lowercase, special character, number, etc.);
5. Be sure the web browser is set for maximum security;
6. Use only vendor security software that updates automatically;
7. Configure your system to monitor unusual events;
8. Participate in subscriber logon at reputable sites only;
9. Do not open emails, attachments or follow links from people you don't know; and
10. Use secure connections when making bank transactions or ordering online.

4.6. (U) Travel / Cover Travel

4.6.1 (U) Cover is an arrangement whereby a U.S. or foreign government organization or person, or a U.S. or foreign private sector entity or individual, provides backstopping for intelligence personnel, installations, or activities. The purpose is to conceal the individual's intelligence sponsorship or affiliation through the use

of the name, organization, facilities, reputation, or credentials of the cover provider. Cover may be used in NRO acquisitions and operations to protect NRO's associations with specific companies, technologies or activities where the relationship itself would be an OPSEC indicator and reveal critical information.

4.6.2 (U) To expedite security screening, in coordination with private industry, the Transportation Security Agency (TSA), developed Registered Traveler (RT) programs. Applicants must provide extensive biographic and biometric data, including employment information to participate in the RT program. Multiple companies administer the RT program by collecting data and maintaining databases of traveler biographic and biometric data. These RT programs are intended to be shared for security coverage worldwide, but the extent of the information shared with foreign countries is unknown. Therefore, persons who travel in cover status may want to carefully consider the potential of cover compromise before they elect to participate in an RT program.

4.6.3 (U) Travelers must also be aware of the fact that many businesses and organizations such as rental car companies, hotels, and airlines keep a record of personal information.

4.6.4 (U) Helpful tips to help maintain cover:

1. Do not use your [redacted] card while on official travel; (b)(3)
2. Do not disclose "nro.mil" or ".ic" e-mail addresses to unauthorized personnel;
3. Never allow anyone to photocopy your CAC card; and
4. When necessary, always identify your employer as [redacted] (b)(3)
   [redacted] (b)(3)

4.6.6 (U) Things to remember for all personnel while traveling:

1. Keep a low profile, dress to blend in;
2. Keep ID on you at all times;
3. Remember program approved cover stories;
4. Avoid work-related conversations;
5. Keep a photocopy of passport and tickets;
6. Learn at least a few phrases in the local language;
7. Carry enough money in local currency to use a pay phone;
8. Go through your carry-on luggage and remove items that may pose an OPSEC risk such as: federal credit union credit cards (especially [redacted] ID's of interest, business cards, information revealing organizational affiliation; (b)(3)
9. Put your laptops and notebooks in your carry-on luggage;
10. Use closed faced luggage tags;

11. Select your cab carefully, only use licensed cabs;

4.6.7 (U) Department of State: Tips for traveling abroad:

1. Register so the State Department can better assist you in an emergency at https://travelregistration.state.gov (UMIS). This will help persons contact you if there is a family emergency in the U.S., or if there is a crisis where you are traveling. In accordance with the Privacy Act, information on your welfare and whereabouts will not be released to others without your authorization;
2. Make sure you have a signed, valid passport, and a visa, if required, and fill in the emergency information page of your passport;
3. Leave copies of your itinerary, passport data page and visas with family or friends, so you can be contacted in case of an emergency;
4. While in a foreign country, you are subject to its laws. The State Department web site at http://travel.state.gov/travel/cis_pa_tw/cis/cis_1765.html (UMIS) has useful safety and other information about the countries you will visit; and
5. Refer to [redacted] for more details on foreign travel threats. (b)(3)

[redacted] (b)(3)

4.7. (U) Identity Protection

4.7.1 (U) Identity theft occurs when someone uses your personal information, like your name, social security number or credit card without your permission to commit fraud or other crimes. Identity theft crimes can happen in many ways, and you may never know you are a victim until you are contacted by a debt collection agency or law enforcement. Identity theft is serious and while some victims can resolve their problems quickly, others can spend hundreds of dollars and numerous hours repairing the damage to their name and credit.

4.7.2 (U) According to the Federal Trade Commission (FTC) nine million individuals have their identity stolen every year in the United States.

4.7.3 (U) What to do if your identity is stolen?

1. (U) Place a "Fraud Alert" on your credit reports and review those reports carefully. Notifying one of the three following nationwide consumer reporting companies is sufficient: TransUnion, Experian and Equifax;
2. (U) Close any accounts that have been tampered with or established fraudulently;
3. (U) File a police report with local law enforcement officials. This is an essential step so that there is proof of a crime in order to claim your rights as a victim; and

4. (U) Report your theft to the Federal Trade Commission, online at www.ftc.gov/complaint (UMIS), or phone by calling 1-877-ID-THEFT (438-4338).

4.7.4 (U) The below site gives a list with links to the websites of organizations that you need to contact and many of the forms needed to help start the process of recovering your identity and credit.

www.onguardonline.gov/topics/identity-theft.aspx (UMIS)

4.7.5 (U) Contact your PSO, who will inform the NRO Personnel Security Division (PSD) of the identity theft.

4.7.6 (U) Tips to Protect Your Identity:

1. Protect your Social Security Number, credit card numbers, bank account information, and driver's license number;
2. Shred all documents with personal information on it including pre-approved credit cards;
3. Destroy digital data by using a software tool to overwrite it;
4. Check your statements for unauthorized charges/events;
5. Limit information on your checks to name and address;
6. Analyze your credit report annually; and
7. Use reputable, well-known internet sites when shopping, and research those you're not familiar with.

4.8. (U) Inadvertent Disclosure of Classified Information

4.8.1 (U) Protection of classified information is vital. All actual or suspected incidents of any compromised SCI or collateral information must be **immediately** reported to your PSO. If you inadvertently remove classified or sensitive information from a SCIF, *Do NOT destroy it.* Protect the information and return it to the SCIF immediately. The PSO will conduct an inquiry to determine if a compromise has occurred, adjudicate the incident, and document it in the Security Log (NRO Incident Database).

4.8.2 (U) Personal discipline is critical:

1. Be aware of your surroundings and what you are talking about;
2. Keep your work area organized;
3. Before faxing or emailing a document via unsecure communications verify that it is unclassified; and
4. Thoroughly inspect your belongings before you leave work.

4.9. (U) Indicators: Distinctive Clothing, Emblems, License Plates, etc.

4.9.1 (U) Indicators are any detectable activity and/or information when observed by itself, or in combination with other information, creates to OPSEC indicators or reveals critical information that can be exploited by an adversary.

4.9.1.1 (U) Distinctive Clothing, Emblems, and Logos:

4.9.1.1.1 (U//~~FOUO~~) The NRO has classified contracts with some industry partners. When traveling to these facilities, you have to be careful about what text, logos and emblems are on your clothing, business cards, stationary, etc. that may reveal a classified association.

4.9.1.1.2 (U) For military personnel, it is good OPSEC to travel in civilian clothes so you don't make yourself a target. For further guidance consult with your PSO.

4.9.1.1.3 (U) The policy on wearing military uniforms varies with OPSEC requirements at the location of classified activities. Prior to visiting a contractor facility, NRO personnel should determine whether wearing military uniforms is appropriate.

4.9.1.2 (U) Signing attendance Sheets:

4.9.1.2.1 (U) With few exceptions, military personnel detailed to the NRO will sign in as their parent military organization (Navy, Air Force, etc.) and not "NRO" when visiting contractor locations in uniform. When not in uniform, personnel must sign in as "Self." Contractors and government civilians must use the same approach and sign in as "Self."

4.9.1.3 (U) License Plates:

4.9.1.3.1.1 (U) We are all proud of our jobs and the contributions we make to the NRO. Some are so proud that they put revealing information on license plates. For example, they put their job title, in which field they work, or that they are affiliated with the NRO, space programs, etc. Vanity plates that reveal critical information about you or your professional activities can peak an adversaries interest and make you a target.

4.10. (U) NRO Launch (NROL)

4.10.1 (U) During Launch Flow:

1. Beware of elicitation techniques in public places (restaurants, bars, etc.);

2. Lauch vehicles typically display the NRO seal – individuals must be aware of what can or cannot be revealed beyond basic "fact-of" an NRO launch;
3. Practice good OPSEC tradecraft;
4. Report any suspicious individuals/incidents to your security officer;
5. Refrain from displaying NRO or launch related logos or badges in public areas;
6. Don't draw attention to yourself while in public areas; and
7. Do not discuss work in public areas.
8. Refer all questions by the public or media to the NRO Office of Corporate Communication (OCC) or launch site Public Affairs (PA); and
9. Even though the launch window is downgraded to U//FOUO 100 days prior, don't discuss specific launch information in public.

4.11. (U) Need-to-Know

4.11.1 (U) You, as an authorized holder of classified or sensitive information, are required to determine an individual's Need-to-Know before you grant him/her access to any classified, sensitive, or critical information within your control. It is your responsibility to confirm that he or she truly needs the information to perform his or her job.

4.11.2 (U) All NRO personnel are responsible for protecting classified, sensitive, and critical information. Your personal responsibilities include using all the security tools available to you, such as secure phones, secure faxes, safes, and badges, and learning the security skills you need to succeed in the National Security environment. One of these skills is the ability to determine Need-to-Know. Failure to apply this principle has resulted in some of the most damaging espionage cases in recent history. Statistically, the Federal Bureau of Investigation (FBI) reports that 80% of espionage is committed by "insiders." Most insiders who committed espionage were fully cleared individuals. In almost every case, these insiders gained access to information not pertinent to their jobs by circumventing the Need-to-Know principle. They were able to do so because their co-workers failed to properly control access to classified, sensitive, and critical information under their control.

4.12. (U) Family and Friends

4.12.1 (U) Keeping potential adversaries from discovering our critical information protects our current and future planned missions. Success depends on secrecy with both classified and sensitive unclassified information so we can accomplish our mission with less risk. Adversaries can gain information from those that support the mission as well as their family members. Make sure that family members understand the importance of protecting information about your employment and travel activities. Telephones, information technology devices, trash, media, e-mail, web pages, virtual worlds, and Social Networking Sites are all ways the adversary may try to elicit information from you and your family.

4.13. (U) Pre-Publication Review

4.13.1 (U) Any material intended for public release that relates to the NRO's mission or activites must be reviewed and approved prior to release. This applies to all NRO employees, government and contractor, currently or formerly assigned to the NRO. Materials include, but are not limited to, electronic release, such as websites, e-mail, or faxes; and publications, such as resumes, books, articles, manuscripts, briefings, and speeches. Drafts must always be created on classified networks to eliminate security and OPSEC concerns.

4.13.2 (U//~~FOUO~~) Each directorate and office has a designated Information Access Officer (IAO). Before submitting a pre-publication request, consult your IAO. If you do not know your IAO, contact the Information Access and Release Team (IART) at (secure) [redacted] or visit: (b)(3)

[redacted] (b)(3)

4.14. (U) Social Networking Sites (SNS)

4.14.1 (U) SNS like Facebook, Twitter, Myspace, etc., are websites and applications that connect people in spontaneous and interactive ways. Rather than using direct point-to-point communication, SNS allow users to publish information as a one-to-many form of communication. While SNS can be useful and fun, they can provide adversaries with critical information needed to harm or disrupt our mission. When information is posted on a SNS or anywhere on the web/internet, it can no longer be considered private. Practicing SNS OPSEC will help individuals recognize critical information and protect it from our adversaries. Always be aware of the image you present when posting anything to a SNS.

4.14.2 (U) Before posting to a SNS ask:

1. Who owns the site?
2. Who are their partners?
3. Where is this site hosted?
4. Who has access to your postings and profile data?
5. Why do they need this information?
6. Does the site sell information to a third party (many SNS are data brokers)?
7. What can an adversary glean from your SNS postings?
8. Is it revealing info about what we do and how we do it?
9. What can be gained by observing your actions or reading what you put online?
10. What is your current web-presence? (Google/Bing yourself – you might be surprised)

4.14.3 (U) Information you must not share on a SNS:

1. Username, passwords, network details;
2. Physical security and logistics;
3. Mission capabilities and limitations; and/or
4. Any details of your relationship with the NRO.

4.14.4 (U) Things you must to consider as OPSEC concerns when posting on SNS:

1. Names and photos of your family and co-workers;
2. Hometown, high school, mother's maiden name (often password recovery security questions);
3. Job title, location, salary, clearances;
4. Schedule and travel itineraries both personal and professional

4.14.5 (U) SNS Best Practices:

1. Make sure your security settings are restrictive as possible and verify them regularly;
2. Verify identities before accepting friend requests;
3. Don't use the same password for everything;
4. Don't rely on the SNS security;
5. Don't run applications from a SNS;
6. Maintain a list of blocked sites for your network;
7. Review your child's online profile and photographs. Children can inadvertently reveal information about their parent's NRO / government affiliation and other personal information.

4.15. (U) SNS Geotagging

4.15.1 (U) Geotagging is the process of adding geographical identification to photographs, video, websites and SNS messages. This data usually consists of latitude and longitude coordinates, though it can also include altitude, bearing, distance, accuracy data and place names. Geotags are automatically embedded in pictures taken with many Smartphones. Most people are unaware of the fact that the photos they take with their Smartphones and uploaded to the Internet have been geotagged. Photos posted to photo sharing sites like Flickr and Picasa can also be tagged with location, but it is not an automatic function.

4.15.2 (U) Digital photos have used geotagging for quite some time. Certain formats such as the JPEG format allow for geographical information to be embedded within the image and then read by picture viewers. This can show the exact location where a picture was taken. Most modern digital cameras do not automatically add geolocation metadata to pictures, but that is not always true. Camera owners should study their camera's manual and understand how to turn off GPS functions. On photo sharing sites, people can tag a location on their photos, even if their camera does not have a GPS function. A simple search for

"Afghanistan" on many photo sharing sites reveals thousands of location tagged photographs that have been uploaded.

4.15.3 (U) The OPSEC community is becoming increasingly concerned about the potential dangers of geotags. Because the location data is not visible to the casual viewer, most people do not realize it is there; and they could be compromising their privacy, if not their safety, when they post geotagged data online.

4.15.4 (U) The geotag function on most smartphones can be disabled. Users should be aware that doing so can sometimes turn off all GPS capabilities, including mapping.

4.15.5 (U) Geotagging OPSEC Concerns:

4.15.5.1 (U) Tagging photos with an exact location on the Internet can allow the adversary to track an individual's location and correlate it with other information. Military, government civilians, and contractors travel to areas all over the world. Some locations are public, others are classified. Individuals must not tag their uploaded photos with a location. Publishing photos of classified locations is detrimental to mission success, and could put people's lives at risk.

4.15.5.2 (U) An example of geotagging OPSEC concerns:

4.15.5.2.1 (U) In August of 2010, a television personality show took a photo of his vehicle using his smartphone. He then posted the photo to his Twitter account including the phrase "off to work." Since the photo was taken by his smartphone, the image contained metadata revealing the exact geographical location of the photo. So by simply posting a photo, he revealed the exact location of his home, the vehicle he drives and the time he leaves for work.

4.15.6 (U) Location-based social networking:

4.15.6.1 (U) Location-based social networking is quickly growing in popularity. Each one of these location based SNS's is different and has its own goals but they all have one thing in common, letting others know about your location and activities. Some of the most popular are:

1. Foursquare, like most location-based social networking applications, focus on "checking in" at various locations to earn points, badges, discounts and other geo-related awards. It is also used to meet friends and new people;
2. Facebook's Places is similar to Foursquare in that it gives an individual's location when the users posts information using a

mobile application. (This function is automatically active on all Facebook accounts until disabled); and

3. Gowalla is a location-based social networking application that functions much like Foursquare and Facebook Places. Users can build a Passport which includes a collection of stamps from the places users have been. Gowalla users can also post photos and submit tips at various locations.

4.15.7 (U) Location-based SNS OPSEC Concerns:

4.15.7.1 (U) Some social networking applications can allow an adversary to track your movements and activities every day. By tracking these movements/activities and aggregating the information an adversary can determine where you live and possibly where you work, making you, your family and your coworkers a potential targets.

4.15.7.2 (U) Remember the main function of location-based social networking applications are to broadcast a user's specific location.

4.16.(U) Trash

4.16.1 (U) Unclassified information of a sensitive nature, improperly handled, can easily provide adversaries with valuable information on current and future operations. Throwing your unclassified trash away may be giving up sensitive information. Dumpster diving or "TRASHINT" is when the adversary collects our trash to gain intelligence about our mission. Be aware of what you throw away in your unclassified trash container; an NRO best practice is to dispose of all written materials, regardless of classification, in a burn bag. At home, shred any sensitive data containing travel arrangements, names, social security numbers, addresses or finances.

4.16.2 (U) Examples of items you must NOT throw in the unclassified trash:

1. Files;
2. Letters;
3. Memos;
4. Photographs;
5. Identification;
6. Passwords;
7. Personal bank account numbers, credit cards, medical records;
8. E-mails/documents that are sensitive but unclassified marked "FOUO";
9. Photocopy of driver's license, travel itinerary, and pay stub; and/or
10. Post-it notes with names and phone numbers of NRO personnel.

5. (U) CONCLUSION

5.1 (U) OPSEC is a process that identifies critical information to determine if friendly actions can be observed by adversaries. It determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

5.2 (U) By employing OPSEC, NRO personnel deny an adversary critical information concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. OPSEC does not replace other security disciplines, it supplements them.

5.3 (U) NRO personnel must incorporate OPSEC into everything we do (at work and away from work). We must all ask ourselves what an adversary could glean from the observables we create. Does it reveal information about what we do and how we do it? Remember, think like the adversary.

5.4 (U) Practicing good OPSEC is essential to NRO mission success.