RECOMMENDATIONS FOR NRO PERSONNEL INTERNET CONDUCT

11 August 2014

(U) Background

(U//~~FOUO~~) The Internet, including Web-based tools and social networking websites, contributes great value to daily life, but also pose security and counterintelligence risks to personal data and other sensitive information. As members of the IC, NRO personnel should recognize and understand these risks. For example:

a. (U//~~FOUO~~) Non-state actors use social networking websites for communication, research, and analysis. Personal data about IC personnel on these websites are vulnerable.

b. (U//~~FOUO~~) Foreign intelligence services actively harvest information about IC employees, locations, and activities from these websites.

c. (U//~~FOUO~~) IC personnel have been the victims of suspicious, sometimes aggressive, activity through social networking websites, including phishing, friend requests, and other unsolicited contact designed to elicit and acquire sensitive or classified data.

(U) Scope and Applicability

a. (U//~~FOUO~~) These recommendations apply to all NRO components and personnel, including government, military, contractor, and assignees to the NRO, but do not restrict authorized activity in support of NRO missions. Please refer questions regarding the applicability of these recommendations to such activity to OGC and the Office of Public Affairs (OPA). References to "you" and "your" in these recommendations indicate all NRO personnel as defined above.

b. (U//~~FOUO~~) NRO personnel should consider these recommendations when using the Internet, including social media, if content may reveal classified or sensitive unclassified information, or identify or in any way characterize the NRO, IC elements or personnel, or intelligence data or activities, whether using personal computers and devices or U.S. Government systems. NRO personnel consent to monitoring of their use of U.S. Government systems. Violators of security regulations may be subject to NRO discipline and criminal prosecution (reference p).

c. (U//~~FOUO~~) Notwithstanding any recommendations in this ND, all NRO personnel must still submit all content intended for public dissemination to the IRRG for prepublication review if it identifies or in any way characterizes the NRO, IC elements or personnel, or intelligence data or activities (reference i). The IRRG will consult the appropriate stakeholders to ensure their concerns are addressed. Examples of public online content that NRO personnel should avoid posting and that would be subject to an IRRG review include, but are not limited to:

a. (U) Blog posts on topics related to the IC;

b. (U) Tweets or posts about your job or performance review;

c. (U) Facebook status updates about your coworkers, supervisor, or NRO leadership;

d. (U) Photographs of NRO or IC facilities;

e. (U) Photographs of NRO or IC personnel, unless taken in a personal capacity and with their prior consent;

f. (U) All resumes or other descriptions of official duties and responsibilities;

g. (U) Biographies that refer to your NRO or IC affiliation, such as for alumni or professional publications; and

h. (U) Launch photos, status, and related activity.

(U) Recommendations for Mitigating Risk:

a. (U) Follow professional standards and conduct, common sense, and sound judgment when using the Internet, Web-based tools, or social media to help mitigate many potential risks.

1. (U) **Protect your online privacy—do not rely on the provider.** Use website features to limit who can see your personal profile(s). The default for most social media websites is that everyone can see your information. When establishing and maintaining a page or profile, consider what information you provide, understand the privacy controls and settings and set them appropriately to protect your information, and routinely validate and update your privacy settings as providers may change them periodically or return them to a default setting when performing system updates. Do not post personal details, such as hometown, high school, mother's maiden name, or personal travel, which make targeting you easier and are often answers to password recovery security questions. You also may choose to limit posting of personal photographs, due to developments in facial recognition technology.

2. (U) **Protect your personal information.** Adversaries, including foreign intelligence services and criminal elements, can, using spyware, malware, phishing, or any number of other methods, obtain personal information from unprotected systems.

a. (U) Any of the following may be stolen from your home computer or other devices without your knowledge:

1. (U) Email logs and content;

2. (U) Software registration records;

3. (U) File structure;

4. (U) Network logons;

5. (U) Cache;

6. (U) Names, addresses, phone numbers, and email addresses of you and your personal contacts; and

7. (U) Credit card numbers, bank accounts.

b. (U) You can further protect your personal information by:

1. (U) Turning off Internet cookies;

2. (U) Regularly updating anti-virus software with new definitions;

3. (U) Using different passwords for each website;

4. (U) Protecting your passwords;

5. (U) Creating accounts using strong passwords that include a mix of uppercase, lowercase, special characters, and numbers;

6. (U) Setting your web browser for maximum security;

7. (U) Using only vendor security software that updates automatically;

8. (U) Configuring your system to monitor unusual events;

9. (U) Participating in subscriber logon at reputable websites only;

10. (U) Not opening emails or attachments or following links from people you do not know;

11. (U) Establishing email spam filters on your personal email account;

12. (U) Using secure connections when making bank transactions or ordering online;

13. (U) Not running applications from a social media website; and

14. (U) Maintaining a list of blocked websites for your network.

3. (U//~~FOUO~~) **Protect your professional identity.** Do not use your nro.mil email address to establish a personal account on a social media platform. Refrain from writing, posting, tweeting, or publishing anything to a personal profile, including photographs, videos, and links to other content, that could needlessly expose your specific affiliation with NRO. Be cautious when joining, following, friending, or liking any person or organization online. Overt NRO personnel may list their employer as the U.S. Government or NRO, but should not specify the NRO office in which they work without clearing it through the IRRG process. NRO personnel under cover should avoid any online behavior that might compromise their cover persona and affiliation and should consult with the [redacted] for additional guidance. (b)(3)

a. (U) Examples of online behavior that NRO personnel should not engage in include, but are not limited to:

1. (U) Friending, liking, posting to, commenting on, reposting from, linking to, or becoming fans of official or unofficial IC agency websites or profiles;

2. (U) Routinely posting or linking to news articles on a particular intelligence topic;

3. (U//~~FOUO~~) Posting photographs of other NRO or IC personnel, unless taken in a personal capacity and with their prior consent; and

4. (U//~~FOUO~~) Posting photographs of NRO or IC facilities and activities.

b. (U//~~FOUO~~) Your personal social media presence, such as on Facebook, LinkedIn, Twitter, blogs, or other Internet usage may provide clues to your government affiliation. A determined adversary can build a picture of your preferences by analyzing your links, individuals and websites you follow, your online friends, blogroll, and other indicators. We all leave an online footprint whenever we use the Web; consider whether your footprint might make you a target. Any statements you make or actions you take online may subject you to legal, ethical, or other repercussions. Carefully consider whether, through your personal communications, you could reveal, undermine, or adversely affect the IC, its operations, or its mission by:

1. (U) Joining certain groups or following participants of a particular debate;

2. (U) Expressing solidarity with certain causes through graphics, icons, badges, or otherwise;

3. (U//~~FOUO~~) Expressly identifying your affiliation with NRO or the IC (although overt NRO personnel may list their employer as the U.S. Government or NRO, consider whether it is appropriate to do so);

4. (U//~~FOUO~~) Sharing information that reflects upon, criticizes, or provides commentary regarding your job, supervisor, or the policies of the U.S. Government, IC, or NRO; or

5. (U) Failing to manage appropriately the various privacy controls and settings offered by each social network provider.

c. (U) Additional considerations when posting photos online:

1. (U) Social networking websites contain facial recognition and tagging tools that can be used on any photographs you post. People in your photos may be identified, thus allowing adversaries to conduct link analysis of your contacts, your contacts' contacts, etc.

2. (U) Geotagging, the embedding of GPS information in the metadata of digital photographs, makes it possible for adversaries and predators to identify the locations you visit based on your posted photographs. The geotag feature on most cameras and smartphones can be turned off.

3. (U) Many website user agreements indicate that information and photographs posted by users become property of the website. Carefully review all agreements to be sure you understand and are comfortable with them.

4. (U//~~FOUO~~) **Protect the professional identities of others.** Your responsibilities to your coworkers extend to all public spaces, both physical and virtual. Your online behavior could lead to unintended consequences for those linked to you. Be cognizant of and help protect the cover status of others. Also, your online friends could be targeted if you expose them through your affiliation with NRO or the IC.

5. (U//~~FOUO~~) **Project a professional impression.** You represent NRO and the U.S Government. Ensure that your profile(s) and all content you post, even if solely personal in

nature, is consistent with how NRO professionals and federal employees should present themselves, does not violate the public trust associated with your position, and conforms to the highest standards of ethical conduct, especially if you identify yourself as a U.S. Government or NRO employee, or have a position for which your association is publicly known.

6. (U//~~FOUO~~) **Do not reveal sensitive information about your job responsibilities.** Do not establish relationships with working groups, professional associations, or IC-related profiles, whether official or unofficial, if doing so would reveal, even inadvertently, classified or sensitive information about your job responsibilities. Carefully research the origins of the online groups and associations you consider joining to be sure you understand their missions and membership.

7. (U//~~FOUO~~) **Exercise sound judgment when performing Internet searches.** Internet searches related to intelligence issues, whether on personal computers and devices or U.S. Government systems, can reveal patterns of activity or behavior to our adversaries, just as your Internet behavior can alert marketers to your consumer preferences.

8. (U//~~FOUO~~) **Avoid mixing your personal and professional lives online.** Colleagues, supervisors, and our adversaries often have access to the online content you post. NEVER disclose non-public government information or post anything else that you would not want them to see.

9. (U) **Be cautious when making friends online.** Verify identities before accepting friend requests or otherwise making associations via the Internet. Foreign intelligence services may attempt to friend IC officers and others as an assessment vehicle and to verify associations with other people, places, or events. Be certain you know with whom you are associating. Remember that foreign contacts and associations, even if only through social media, must be reported to your program security officer (PSO).

10. (U) **Report your concerns.** If you see or experience suspicious activity on a social networking website, if suspicious individuals repeatedly attempt to contact you, or if you have any questions about possible security issues associated with your social networking presence, contact your PSO and the OS&CI [redacted] via secure phone or NROnet. Do NOT try to identify suspicious individuals or attempt to contact them without guidance from appropriate NRO authorities. (b)(3)

11. (U) **Educate your family members.** Discuss with family members their online profiles, social networking activities, and the information they provide. Be sure they recognize potential threats to your professional identity, personal data, and privacy. Verify that your children's online profiles and photographs do not inadvertently reveal your work or personal information.

12. (U//~~FOUO~~) **Do not indicate NRO or IC approval.** Do not suggest official approval by NRO or other IC elements in your personal postings. Do not use logos, seals, or official acronyms that identify NRO or other IC elements in any posts, graphics, usernames, handles, or screen names.

13. (U//~~FOUO~~) **Report any media interaction.** Promptly refer all news media inquiries relating to NRO or the IC, including from bloggers or Internet media sources, to OPA.

14. (U//~~FOUO~~) **Know that information on the Internet is permanent.** Regardless of how you use the Internet, all of your online activity (postings, search engine terms, social networking activities, and browsing habits) will remain in the cyber world forever and may be analyzed for malicious purposes. Once information or photographs are published online, they are part of a permanent record, even if you later remove or delete them or attempt to make them anonymous. Before posting anything, you should consider:

a. (U) Who owns the website?

b. (U) Who are their partners?

c. (U) Where is this website hosted?

d. (U) Who has access to your postings and profile data?

e. (U) Why do they need this information?

f. (U) Does the website sell information to a third party? (Many websites are data brokers)

g. (U) What can an adversary glean from your postings?

h. (U) Do your postings reveal information about what NRO or the IC does and how?

i. (U) What can be gained by observing your actions or reading your input online?

j. (U) What is your current web presence? (Perform a web search on yourself—you might be surprised.)

b. (U//~~FOUO~~) These recommendations will help you limit potential damage from social networking, online publishing, and general Internet use. As an IC professional, you should understand security and counterintelligence threats, and ensure that your online behavior does not harm you, your colleagues, the NRO or other U.S. government organizations, or the United States.

c. (U) Questions about these recommendations should be directed to OPA.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu