OPA Facebook/Social Media Educational Announcements
2-9 July 2014

T Noon – 1 July
M Morn – 2 July
M Noon – 2 July

NRO's Official Facebook Page is Coming This Summer!

(U) The launch of NRO's official Facebook page has been postponed from 2 July, but is anticipated for later this summer. The page will provide greater transparency, and allow NRO to better share our unclassified history, missions, and successes with the public.

(U) To mitigate potential risks, NRO personnel should not "like," follow," or "share" posts from the NRO Facebook page or other IC social media sites, nor accept "friend" requests from any sites claiming to represent elements of the IC.

(U//~~FOUO~~) All NRO personnel should observe common sense and good judgment when using NRO's Facebook page or any social media site. Avoid revealing your NRO or IC affiliation online, or sharing any details that might indicate your affiliation.

(U) Please see the attachment, *Recommendations for NRO Personnel Internet Conduct*, for additional guidance and recommendations.

Th Morn – 3 July
T Noon – 8 July

NRO's Facebook — Understand the Risks

(U) With the anticipated launch of NRO's official Facebook page this summer, NRO personnel, as members of the Intelligence Community (IC), should recognize and understand potential risks.

(U//~~FOUO~~) The Internet, including Web-based tools and social networking sites, contributes great value to daily life, but also pose security and counterintelligence risks to personal data and other sensitive information. For example:

a. (U//~~FOUO~~) Non-state actors use social networking websites for communication, research, and analysis. Personal data about IC personnel on these sites 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 sites, including phishing, "friend" requests, and other unsolicited contact designed to elicit and acquire sensitive or classified data.

(U) Please see the attachment, *Recommendations for NRO Personnel Internet Conduct*, for additional guidance and recommendations.

Th Noon – 3 July
T Morn – 8 July

Facebook and Prepublication Review

(U//~~FOUO~~) In anticipation of the launch of NRO's official Facebook page this summer, all NRO personnel are reminded that they must submit all classified and unclassified content intended for 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. The IRRG will consult the appropriate stakeholders to ensure their concerns are addressed.

(U) Examples of public online content ***that you should normally 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 or boss;
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) Please see the attachment, *Recommendations for NRO Personnel Internet Conduct*, for additional guidance and recommendations.

M Morn – 7 July
W Noon – 9 July

Are You Safe on Facebook? Protect Yourself and Your Colleagues on Social Media

(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. Here are just a few ways to keep safe:

(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 sites 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.

(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.

(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)

(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.

(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.

(U) Please see the attachment, *Recommendations for NRO Personnel Internet Conduct*, for additional guidance and recommendations.

M Noon – 7 July
W Morn – 9 July

What Else Can I Do to Stay Safe on Facebook and Social Media?

(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.

(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.

(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.

(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).

(U) **Report your concerns.** If you see or experience suspicious activity on a social networking site, 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. (b)(3)
Do NOT try to identify suspicious individuals or attempt to contact them without guidance from appropriate NRO authorities.

(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.

(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.

(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.

(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. (Perform a web search on yourself—you might be surprised.)

(U) Please see the attachment, *Recommendations for NRO Personnel Internet Conduct*, for additional guidance and recommendations.