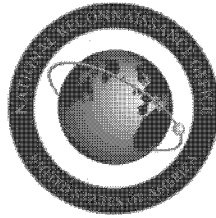


**National Reconnaissance Office**  
Business Function 110, Strategic Communications  
**Directive 110-6, Public Affairs Social Media Use**

---



12 SEPTEMBER 2014

---

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

TABLE OF CONTENTS

(U) ND 110-6 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.....6  
(U) SECTION VI - DIRECTIVE POINTS OF CONTACT.....12  
(U) APPROVING SIGNATURE.....12  
(U) APPENDIX A - GLOSSARY.....13  
(U) APPENDIX B - RECOMMENDATIONS FOR INTERNET CONDUCT.....14

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

(U) ND 110-6 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

**(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) 110. 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, activities, and roles and responsibilities for how NRO, the Office of Public Affairs (OPA), and the Office of Congressional and Public Affairs (OCPA) shall conduct social media.

**(U) SECTION II - APPLICATION**

(U) All NRO personnel who perform tasks or have duties specific to NBF 110 shall comply with this ND and its corresponding instructions. When 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) President's Memorandum on Transparency and Open Government, 21 January 2009
- b. (U) Privacy Act of 1974, as Amended (5 United States Code 552a)
- c. (U) NRO Governance Plan, 25 October 2011
- d. (U) NBF 110, Strategic Communications, 3 April 2012
- e. (U) NRO Directive (ND) 50-7, Appropriate Use of NRO Information Technology, 7 March 2012
- f. (U) ND 100-28, NRO Information Enterprise Account Authentication Policy, 30 August 2012
- g. (U) ND 55-1, Information Privacy, 7 May 2013

**ND 110-6, Public Affairs Social Media Use  
FY 2014**

---

h. (U) ND 55-2, Privacy Breach and Complaint Management, 7 May 2013

i. (U) NRO Instruction (NI) 56-2-2, Prepublication Review, 26 February 2013

j. (U) NI 55-2-1, Privacy Breach and Complaint Reporting, 2 May 2013

k. (U) Department of Defense (DoD) Instruction 5400.13, Public Affairs (PA) Operations, 15 October 2008

l. (U) Guidelines for Secure Use of Social Media by Federal Departments and Agencies, Version 1.0, Federal CIO Council, September 2009

m. (U) Directive-Type Memorandum 09-026 - Responsible and Effective Use of Internet-based Capabilities, Deputy Secretary of Defense, 25 February 2010

n. (U) Intelligence Community (IC) Standard 500-16, Password Management, Office of the Director of National Intelligence (ODNI), 16 March 2011

o. (U) IC Directive 205, Analytic Outreach, ODNI, 28 August 2013

p. (U) FORM 4414, Non-Disclosure Agreement, December 2013

**(U) SECTION IV - POLICY**

a. (U) OPA within the Business Plans and Operations Directorate (BPO) shall establish and maintain an NRO presence on selectively chosen unclassified social media websites. The NRO's presence on the chosen websites shall always be open and acknowledged.

b. (U) NRO's official unclassified social media presence and activities shall support NRO strategic communication goals, increase public awareness and understanding of the NRO, reinforce the NRO's unique role in the IC, and help align NRO with the President's Memorandum on Transparency and Open Government, January 21, 2009.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

c. (U) NRO's social media presence shall follow DoD-approved contracts with the respective social media providers.

**(U) SECTION V - ROLES AND RESPONSIBILITIES**

**(U) Management of Social Media Accounts and Web Applications**

a. (U) The Director or Deputy Director of OPA (D/OPA or DD/OPA) shall approve access for social media managers to maintain NRO's selected social media websites and to use Web applications (apps) that support social media activities. The Office of Security and Counterintelligence (OS&CI) shall conduct a security file review of social media managers before they are granted access as privileged users of NRO website accounts. OPA shall limit the number of managers to the minimum necessary to properly administer the NRO's social media websites and shall review and validate the managers' need for access annually.

b. (U) Social media managers shall monitor and maintain social media accounts and Web apps, including removing access to social media accounts upon the departure, transfer, or termination of a social media manager.

c. (~~U//FOUO~~) Social media managers shall access NRO social media websites only from NRO Unclassified Management Information System (UMIS) workstations to review or post content to a website.

d. (~~U//FOUO~~) When required by policy (reference i), or when D/OPA, DD/OPA, D/OCPA, or DD/OCPA deem appropriate and applicable, OPA shall consult OS&CI and the Chief Information Office (CIO) before posting data and information on the Internet to ensure there are no security, prepublication, or Privacy Act concerns.

e. (U) OPA shall coordinate with the OP&S  before posting any content containing domestic imagery. (b)(3)  
(b)(3)

f. (~~U//FOUO~~) OPA shall coordinate the creation of any social media website account and its capabilities, features, or add-on enhancements with OS&CI and the Office of General Counsel (OGC) prior to implementation to conduct a security risk assessment and to obtain approval for usage.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

**(U) Password Protection**

a. (U) Social media managers shall use only one shared account for each social media website, but shall employ a credential management service, once such service has been approved by OS&CI. This shall ensure individual access and accountability for each social media manager posting to NRO social media websites. Prior to the acquisition of such services, managers shall document their individual activities on each website.

b. (U) Social media managers shall use strong passwords that follow ND 100-28 or current ND on record to the extent allowed by each website. Managers must be compliant with proper operating procedures for access and use of the NRO Information Enterprise (NIE) at all times.

c. (U) Social media managers shall maintain awareness of the individual sites and change passwords if the owning organization changes security settings or a breach of site security becomes known.

**(U) Access Control**

(U) NRO social media managers shall access NRO websites via UMIS workstations only. Managers shall not use personal social media accounts to manage NRO social media websites or to perform any official NRO social media activities. Managers shall use only the unclassified  email address for all NRO social media accounts.

(b)(3)

**(U) Content**

a. (U) In accordance with NRO policy (reference i), or when D/OPA, DD/OPA, D/OCPA, or DD/OCPA deem necessary, social media managers shall ensure that the CIO Information Management Services Office Information Review and Release Group (IRRG) reviews content shared via social media prior to release through social media to verify that it is publicly releasable. The IRRG shall consult the appropriate stakeholders to ensure that their concerns are addressed and shall review content submissions as quickly as possible.

b. (U) Social media managers shall work with content producers to ensure, to the best of their ability, that all

**ND 110-6, Public Affairs Social Media Use  
FY 2014**

---

content is accurate, relevant, and does not reflect adversely on the NRO, the IC, or the federal government.

c. (~~U//FOUO~~) Social media managers shall ensure that classified information is not posted to or transmitted over the open Internet.

d. (~~U//FOUO~~) All personnel involved in NRO social media shall also ensure that proprietary, privileged, sensitive unclassified, and FOUO information is not transmitted over the unclassified Internet. Always use classified information systems for the transmission of such information. Examples of such information include, but are not limited to:

1. (U) Information concerning official travel;
2. (U) The identities of participants in meetings or conferences that are not open to the general public;
3. (U) Photographs of conference attendees at events that are not open to the general public;
4. (U) Username, passwords, and network details;
5. (U) Physical security and logistics;
6. (U) Mission capabilities and limitations; and
7. (U) Details of employees relationships with the NRO.

**(U) Release Authority**

(U) D/OPA or DD/OPA are the release authorities for content published on NRO social media websites, even if the material has been approved for public release for other purposes. However, when D/OPA, DD/OPA, D/OCPA, or DD/OCPA deem necessary, content, in addition to IRRG review, shall be vetted through OS&CI and CIO and reviewed by D/OCPA or DD/OCPA before posting.



ND 110-6, Public Affairs Social Media Use  
FY 2014

---

**(U) Incident Reporting**

a. (U) NRO OPA personnel shall immediately report all known or suspected computer security events, incidents, and known or suspected data spills to the [redacted] and the OS&CI [redacted]

(b)(3)

(b)(3)  
(b)(3)

b. (U) NRO OPA personnel shall immediately report all known or suspected privacy breaches to the CIO.

c. (U) If an event or incident occurs, all involved NRO personnel and components shall support and assist [redacted] OS&CI, and the NRO Privacy Program (NPP) personnel with whatever assistance they request to conduct damage assessments, implement containment and eradication procedures, and any other actions required throughout the incident investigation and clean up.

d. (U//~~FOUO~~) [redacted] and the OS&CI [redacted] shall provide guidance for containing the incident, for eradicating the cause of the incident, and for restoring the social media website and account to pre-incident operational status. OPA personnel shall not post or delete content from the social media website and account involved in a security incident and shall preserve all evidence until the investigation is complete.

(b)(3)

e. (U) If a social media account is attacked, hacked, or otherwise altered in any way without authorization, [redacted] may authorize OPA personnel to contact the vendor immediately to regain control of the account or restore the page.

(b)(3)

**(U) Interactivity and Monitoring**

a. (U) In managing the NRO's social media websites, the social media managers shall not follow, like, or otherwise endorse any non-U.S. government or commercial social media website unless specifically authorized to do so by D/OPA. Following other U.S. government social media websites is permitted.

b. (U) Social media managers may, with D/OPA or DD/OPA approval, share content created by a governmental or non-governmental third party that relates to NRO if the materials have been approved for public release and are unclassified. This may include posting quotations from previously approved

**ND 110-6, Public Affairs Social Media Use  
FY 2014**

---

content; republishing news headlines or brief descriptions of articles or events; and creating simple summaries of articles, videos, or audio files within applicable copyright laws. Managers may include appropriate introductory or editorial content introducing, describing, or explaining these materials.

c. (U) Social media managers shall seek to prevent public comments and hide or remove any public comments that are posted. Social media managers shall not directly respond to public comments made on NRO social media websites. If deemed appropriate by D/OPA or DD/OPA, managers may submit or share additional content that addresses the subject matter of a comment without directly referencing the comment or commenter.

d. (U) Social media managers shall monitor all content in accordance with the "Abuse" section of this document. Social media managers shall hide or remove any materials or content deemed inappropriate or abusive. If sensitive or classified information is posted to a website from any source, social media managers shall follow the procedures outlined in the "Incident Reporting" section of this document.

e. (U//~~FOUO~~) The OS&CI [ ] shall employ auditing software to monitor and help identify potentially inappropriate, abusive, sensitive, or classified information. The OS&CI [ ] shall notify social media managers of any inappropriate or abusive material, which social media managers shall hide or remove. If the OS&CI [ ] discovers sensitive or classified materials on a website, the branch shall immediately implement its response procedures and notify the social media managers and BPO program security officer (PSO).

(b)(3)  
(b)(3)  
(b)(3)  
(b)(3)

**(U) Counterintelligence**

a. (U//~~FOUO~~) Social media managers shall immediately report to [ ] and the OS&CI [ ] any activity or posting on an NRO social media website suspected to have originated from a foreign intelligence or security service, terrorist organization, or other entity that may be threatening, collecting information, attempting to recruit U.S. persons or influence operations, or conducting illicit activities against the social media website.

(b)(3)

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

b. (U) OS&CI shall review any activity or posting believed to communicate a threat and, if necessary, report it to the appropriate counterintelligence or law enforcement agencies.

c. (U) Social media managers shall notify the OS&CI [redacted] [redacted] of the discovery of any unauthorized social media website purporting to represent the NRO. The social media managers shall then contact and engage the website provider to remove the unauthorized website.

(b)(3)

**(U) Privacy**

a. (U) Each third-party social media website maintains its own privacy policy. Any NRO interaction with a third-party website is subject to that website's privacy policy.

b. (U) The NRO's use of social media shall comply with statutory, regulatory, and policy requirements (references b, g, h, and j) protecting personally identifiable information (PII) and records covered under the Privacy Act. OPA shall coordinate with NPP before posting materials that may contain PII to social media websites.

c. (U) NRO social media websites shall link to and from the NRO.gov website. Anyone selecting an NRO social media website using a link from the NRO.gov website shall receive a notice that the individual is leaving the NRO.gov public website for a non-government hosted, third-party website.

**(U) Media Contacts**

(U) Social media managers shall refer any media queries originating on or through NRO social media websites to D/OPA or DD/OPA.

**(U) Abuse**

(U) Social media managers shall hide or remove any material or content deemed inappropriate or abusive.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

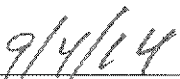
**(U) SECTION VI - DIRECTIVE POINTS OF CONTACT**

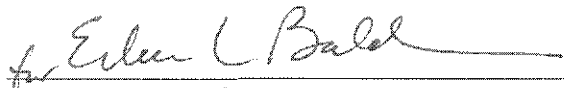
(U) D/OPA and DD/OPA are the main points of contact for any policy and/or process questions associated with NRO social media or related to the implementation and operation of this Directive.


**(U) APPROVING SIGNATURE**

(U) As the NBF owner for Strategic Communications, I confirm that this document provides a complete representation of ND 110-6, Public Affairs Social Media Use, and that the document has been coordinated with stakeholders in this process.

  
\_\_\_\_\_  
Todd B. Peckins  
Strategic Communications,  
NBF Owner

  
\_\_\_\_\_  
Date /

  
\_\_\_\_\_  
Damon R. Wells  
Director, Office of Policy  
and Strategy

  
\_\_\_\_\_  
Date

ND 110-6, Public Affairs Social Media Use  
 FY 2014

**(U) APPENDIX A - GLOSSARY**

<b>Term</b>	<b>Definition</b>
<b>(U) Content</b>	(U) Any text, audiovisual, or multimedia materials shared or posted on a social media website. Examples of NRO content may include: <ul style="list-style-type: none"> <li>a. Historical materials produced by or for the NRO's Center for the Study of National Reconnaissance (CSNR),</li> <li>b. Selected launches of NRO space vehicles, and</li> <li>c. Announcements of a new Director, Principal Deputy Director, or Deputy Director of the NRO.</li> </ul>
<b>(U) Domestic Imagery</b>	(U) Imagery covering the fifty United States, the District of Columbia, U.S. territories, and possessions, including all areas extending twelve nautical miles seaward from a U.S. land mass used for official NRO purposes.
<b>(U) NRO Personnel</b>	(U) For purposes of this document, the following are considered NRO personnel: all military, government, and contractor employees of or assignees to the NRO.
<b>(U) Official Release</b>	(U) A record or document that will be released by the NRO or an NRO component as part of its mission and function.
<b>(U) Prepublication Review</b>	(U) The process established to control and monitor the release of unclassified information about, or affecting the plans, policies, programs, or operations of the NRO, the IC, or the U.S. Government.
<b>(U) Social Media</b>	(U) The collective use of online platforms, applications, and technologies used to share information, and create interactive content beyond static websites. Social media includes social networking websites, video hosting websites, weblogs, and other Internet forums.
<b>(U) Social Media Managers</b>	(U) The OPA-approved administrators of NRO's social media websites and accounts.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

**(U) APPENDIX B - RECOMMENDATIONS FOR INTERNET CONDUCT**

**(U) Purpose**

(U) Appendix B provides NRO personnel recommendations on appropriate Internet use. NRO personnel should regularly review the latest version of these recommendations, which will be amended as technology develops and/or policies change.

**(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,

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

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.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

**(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.



ND 110-6, Public Affairs Social Media Use  
FY 2014

---

- 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.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

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] [redacted] for additional guidance.

(b)(3)  
(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:

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

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.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

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 PSO.

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

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?

ND 110-6, Public Affairs Social Media Use  
FY 2014

---

- 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.