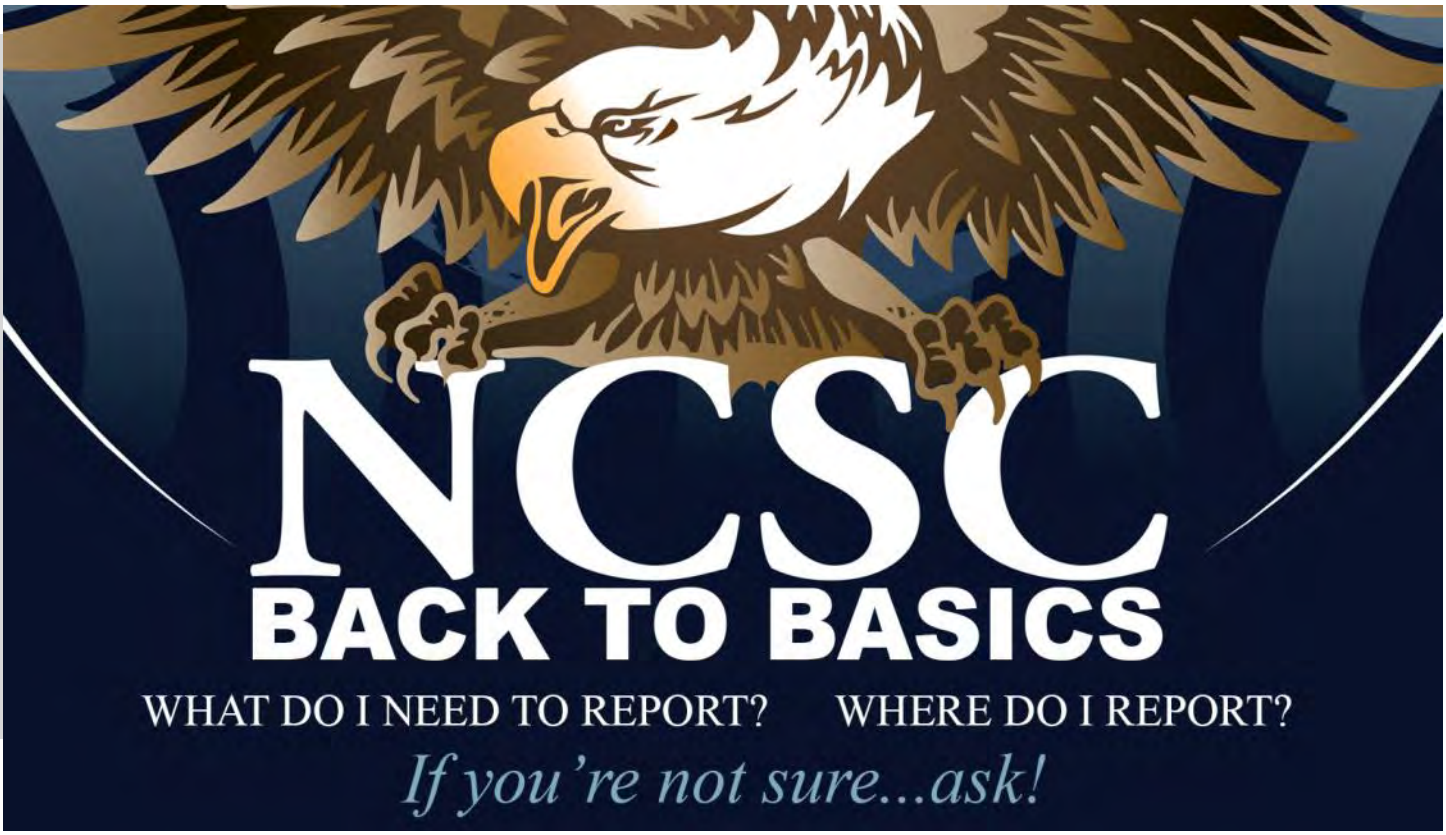
Federal Partner Newsletter

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Volume 1 | Issue 2
July 2019



Protecting Your Personal Information

Bobby Alexander, Social Security Administration

When it comes to personal information, what federal agency is entrusted with the personally identifiable information (PII) of more Americans than the Social Security Administration (SSA)? Safeguarding such highly sensitive information that is so valuable to so many people is one of SSA's highest priorities. In fact, this year we adopted the theme "Share with Care: Respecting Privacy, Safeguarding Data, and Enabling Trust."

Because SSA collects and maintains some of the public's most sensitive data, we have an unwavering commitment to safeguarding this information to the greatest extent possible so we can maintain public trust. In today's world of constantly changing technology, we must be at the forefront of protecting PII while continuing to deliver high-quality Social Security services to our customers. To meet the public's evolving needs, we continue to improve our programs and online services, while implementing new technologies and processes. In doing this, we continue to make privacy safeguards, considerations, and

the overall protection of PII an area of upmost importance. Our commitment is as solid in 2019 as it was when Social Security began in 1935, and we strive daily to ensure the highest level of privacy protections possible.

Reporting Requirements

Mark Frownfelter, Deputy Assistant Director, Special Security Directorate (SSD)

Individuals who hold SCI access have special responsibilities and obligations to report, in advance, on activities, conduct or employment, which could conflict with their ability to protect classified information from unauthorized disclosure or counterintelligence threats. All persons granted access to IC-controlled access programs, including SCI , must comply with specific reporting requirements covered in the Security Executive Agent Directive 3 (SEAD 3), *Reporting Requirements for Personnel with Access to Classified Information or who Hold Sensitive Information*. Those individuals are responsible for ensuring that the reporting requirements are satisfied within the various areas where information is required. This information can be reported through several different avenues and procedures, and may vary from one agency to another. The responsibility is on the individual to ensure the relevant information is properly reported. Overall areas that require reporting include, but may not be limited to, the following:

Unofficial Contact with Foreign Nationals: Regulations require employees to report close and continuing contact with foreign nationals. The mission and responsibilities of federal agencies are such that relationships with foreign nationals may potentially make employees vulnerable to physical, mental, or other forms of coercion by a foreign power or a non-governmental group.

Cohabitation or Marriage to a Foreign National: The marriage of clearance holders to foreign nationals is a subject of potential security and counterintelligence concern. All persons, without regard to their grade or position, contemplating cohabitation/marriage to a foreign national, will be subject to review. On a case-by-case basis, determinations will be made as to how extensive the checks will be on the foreign national.

Personal Foreign Travel: Clearance holders, who are planning private, unofficial travel to a foreign country, are required to report such travel in advance of departure.

Suspected Criminal Activity: Any arrests, pending charges or criminal activity must be reported immediately. Failure to report any criminal activity or incident could lead to serious disciplinary actions, which may include revocation of clearances and/or termination of employment.

Change in Martial Status

Outside Activities, to include:

- Outside employment
- Non-official publications or presentations
- Contact with the media
- Foreign adoption
- Unofficial visits to foreign embassies and missions
- Sponsorship of foreign nationals (to include relatives)
- Participation in political activities (Hatch Act)
- International conferences/academic institutions
- Court/jury duty, legal action, contact with law enforcement
- Overseas operation of citizen band/amateur radio

Training Program

Dana Rainey, Security Liaison and Training Manager, SSD

NCSC's Security Training Program is dedicated to educating those in security or security-related disciplines on Intelligence Community Directives (ICDs) and Security Executive Agent Directives (SEADs) in its course offerings of ICD 704 Personnel Security, ICD 705 Physical Security, and the Special Security Officers Course.

The ICD 704 Personnel Security course trains security specialists (i.e. adjudicators, investigators, polygraphers) on the methods of conducting adjudications to determine eligibility for initial or continued access to classified national security information, or eligibility to hold a sensitive position (national security eligibility determinations).

The ICD 705 Physical Security course prepares officers carrying out the physical and technical security standards that apply to Sensitive Compartmented Information Facilities (SCIFs) and the requirements of the ICD 705 series documents (ICD 705, ICS 705-1, ICS 705-2 and the ICD 705 Technical Specifications).

The Special Security Officers Course (SSOC) provides security professional knowledge of a blend of security disciplines to enhance their ability to identify, assess, mitigate, and resolve security and counterintelligence-related issues; and, support to the mission requirements of their organizations.

To find out more information about these course offerings or to register, contact the registrar at NCSC-Training@dni.gov .

Cyber Security

Lourdes A., NCSC Federal Partner Liaison

Back to Basics includes remaining vigilant to cyber threats and practicing good cyber hygiene. Below are a few suggestions to help you stay safe online, both at home and at work:

Spear-phishing is a common technique used to compromise computer networks and gain access to information. You may receive a seemingly real or official-looking email, text message, or pop-up window to lure you into clicking on a link or attachment.—***Never click on suspicious links or attachments.***

Social media provides bad actors with a platform to target you. Be careful what you share about yourself, your family, and your work, as it can draw unwanted attention from adversaries. The more personal data you post, the more vulnerable you become. —***Maximize your privacy settings and be careful what you share on social media. Never accept friend requests from those you don't know.***

Mobile apps that you download or access via your phone or other device should be used with caution. Apps can track where you are and where you go. Many can access the information on your phone, such as contact lists and other data, and monitor your online activity.—***Research apps before downloading them; know what personal information they are accessing; manage app permissions; and, use an antivirus app.***

Home connected devices—such as home personal assistants, smart TVs, security cameras, and

thermostats —all add convenience but can make you vulnerable, given that many are insecure.—***Change the default password on these devices, update the software regularly, and secure the wireless network you use to connect to these devices. Always adopt strong passwords and use two or three-factor authentication.***

From the Director

William R. Evanina
NCSC Director

With the onset of the summer season, it is a good time to get "Back to Basics." From safeguarding personal information, to adhering to reporting requirements, to maintaining good cyber hygiene, we each have to comply with the high standards of conduct required of persons holding positions of trust. Our adversaries have become adept at targeting U.S. interests, and an individual may be deceived into advancing our adversaries' objectives without knowingly doing so.

Remain vigilant, adhere to best practices and, if you have any personal or professional concerns related to yourself or your colleagues, remember to get back to basics and learn what options you have to obtain assistance.

We hope you continue to find this newsletter to be a valuable source of information and another way for us to remain connected. If you have any suggestions, articles you would like to submit, or other thoughts on how we can enhance our engagement with federal partners, please let us know at ***NCSC_FEDS@dni.gov***.

For more information on NCSC and counterintelligence and security topics, including the supply chain, please visit our website at **https://www.*NCSC.gov*** or follow us ***@NCSCgov on Twitter.***

William Evanina

"As clearance holders and guardians of our nation's security, we are held to the highest standards. We must never take this privilege for granted, and must always adhere to the requirements and regulations that govern this responsibility."