UNITED STATES DEPARTMENT OF COMMERCE
Deputy Assistant Secretary for Intelligence and Security
Office of Intelligence and Security
Washington, D.C. 20230

June 22, 2023

TO: Department of Commerce Cleared Federal Advisory Committee Members

FROM: Nicholas M. Schnare
Director for Security
Office of Security

NICHOLAS SCHNARE
Digitally signed by NICHOLAS SCHNARE
Date: 2023.06.23 08:03:24 -04'00'

SUBJECT: Guidance on Clearance Holder Reporting and Training Requirements

REFERENCES

- Department of Commerce Manual of Security Policies and Procedures, January 2023
- Department Organization Order 20-6, Director for Security, November 2022
- E.O. 13526, Classified National Security Information, January 2010
- 32 CFR Parts 2001 and 2003, Classified National Security Information, June 2010
- Security Executive Agent Direct (SEAD) 3, Reporting Requirement for Personnel Who Access Classified Information and Hold a Sensitive Position, June 2017
- Department of Commerce Memorandum, Implementation of Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, September 2021
- Foreign Travel Briefing Program Handbook, November 2022
- Federal Advisory Committee Act (FACA) (5 U.S.C. § 1001 *et seq*.)

PURPOSE

This memorandum provides guidance for non-Department of Commerce (Department) employee Federal Advisory Committee (FAC) members, appointed by the Department pursuant to the Federal Advisory Committee Act (FACA), for whom the Department has sponsored the member's security clearance (applicable FAC members). This guidance details requirements for applicable FAC members pursuant to Security Executive Agent Directive (SEAD) 3 and the mandatory initial and annual Classified National Security Information (CNSI) training for FAC members holding such security clearances.

BACKGROUND

The Office of the Director for National Intelligence (ODNI) issued SEAD 3, effective June 12, 2017. On September 14, 2021, the Department implemented SEAD 3 for all covered individuals through the issuance of the policy document, *Implementation of Security Executive Agent Directive 3, Reporting Requirement for Personnel with Access to Classified Information or Who Hold a Sensitive Position*. This document outlines reporting requirements for covered individuals for certain activities, such as foreign travel or financial anomalies, to ensure the protection of Classified National Security Information (CNSI). Further, it outlines how covered

individuals incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the United States and abroad.

REPORTING REQUIREMENTS

In accordance with SEAD 3 and the Department's implementation guidance, applicable FAC members with security clearances as described above shall report all activities as outlined in the directive. However, it is understood that reporting procedures required by the Department might not be achievable for such FAC members because of a lack of access to the Department's intranet. Therefore, applicable FAC members that do not have access to SITRepP, the Office of Security (OSY) website portal for reporting, shall report all reportable activities as required in SEAD 3 to Reporting@doc.gov.

TRAINING REQUIREMENTS

Applicable FAC members must sign a SF-312 Nondisclosure Agreement (Attachment 1) and follow instructions for completion and submission (Attachment 2). Additionally, eligible FAC members must receive initial and annual refresher training on the protection of CNSI. The Department's web-based "Annual NSI Security Clearance Holder Training" will satisfy training requirements for applicable FAC members who have access to the Department's intranet. For those without access to the Department's intranet or who would prefer an instructor led training, "Annual NSI Security Clearance Holder Training" will be provided by OSY on a quarterly basis and will satisfy both initial and annual refresher training requirements. Other training besides the "Annual NSI Security Clearance Holder Training," will not be accepted unless provided by OSY.

For FAC members who have access to the intranet, the web-based training does not automatically record completion of the session. The only proof of training is the certificate of completion received after successfully completing the assessment at the end of the training evaluation.

To complete the process to receive credit for the training, the FAC member should:

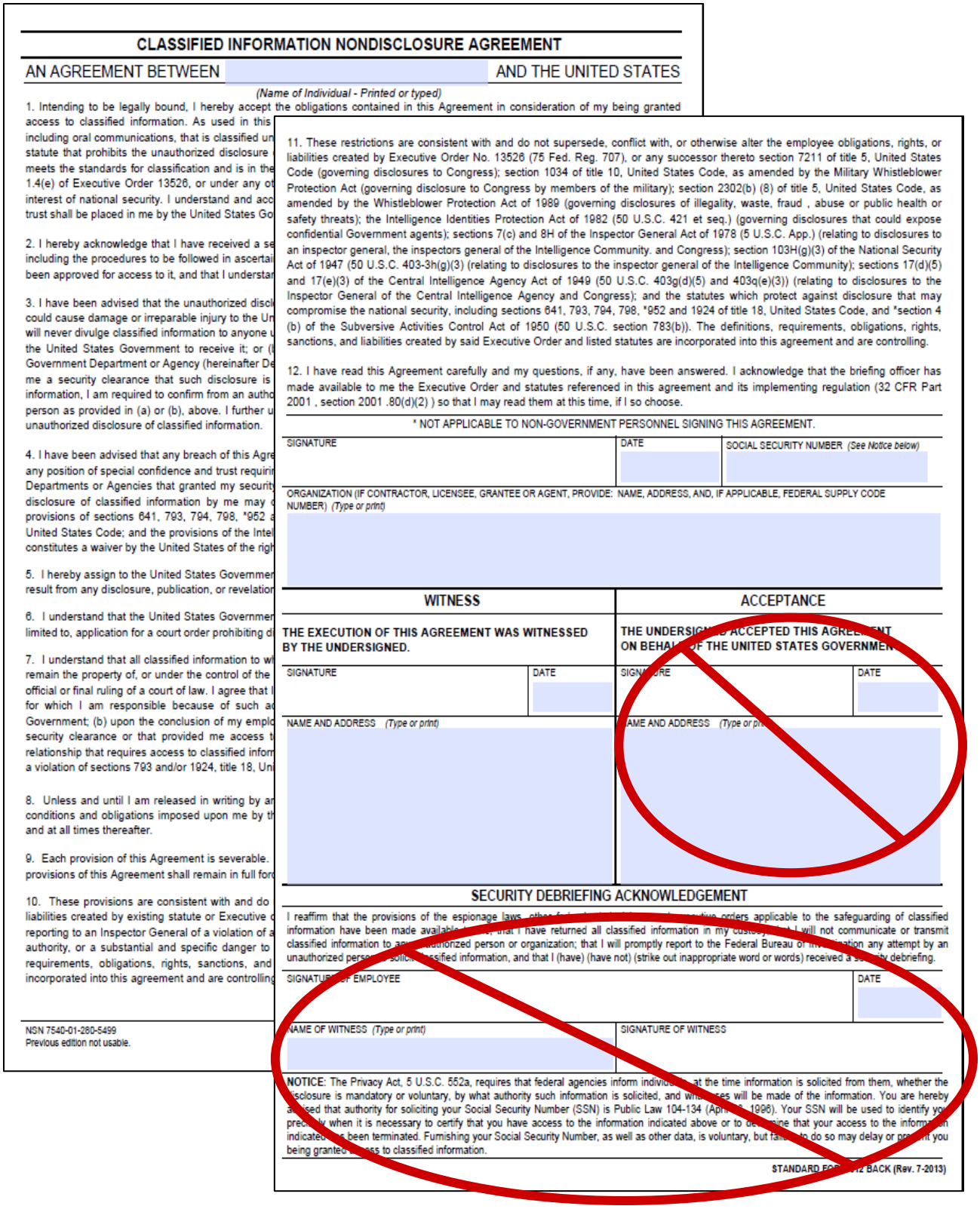
1. Enter his or her full name and other information to be displayed on the FAC member's certificate on the Validation Instructions page (Attachment 3).
2. Once submitted, review the Certificate of Completion (Attachment 4).
3. Convert the Certificate of Completion to a pdf for digital signature or print it for a wet ink signature (Attachment 4).
    a. Note: a wet signature is required unless you have a Department-issued Personal Identity Verification (PIV) card.
4. Once signed, submit the training certificate and your full legal name to OSY_Infosec@doc.gov for training credit in Security Manager, the Department security system of record.

Questions regarding this memorandum may be addressed to the OSY, Information Security Division (ISD) at OSY_Infosec@doc.gov.

Attachments:

1) SF-312 Nondisclosure Agreement Example
2) SF-312 Nondisclosure Agreement Instructions
3) Web-based training Validation Instructions
4) Web-based training Certificate of Completion

Attachment 1: SF-312 Nondisclosure Agreement Example



CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this including oral communications, that is classified un statute that prohibits the unauthorized disclosure meets the standards for classification and is in the 1.4(e) of Executive Order 13526, or under any ot interest of national security. I understand and acc trust shall be placed in me by the United States Go

2. I hereby acknowledge that I have received a se including the procedures to be followed in ascertai been approved for access to it, and that I understar

3. I have been advised that the unauthorized discl could cause damage or irreparable injury to the Un will never divulge classified information to anyone u the United States Government to receive it; or (Government Department or Agency (hereinafter De me a security clearance that such disclosure is information, I am required to confirm from an autho person as provided in (a) or (b), above. I further u unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agre any position of special confidence and trust requirir Departments or Agencies that granted my securit disclosure of classified information by me may provisions of sections 641, 793, 794, 798, *952 United States Code; and the provisions of the Intel constitutes a waiver by the United States of the righ

5. I hereby assign to the United States Governmer result from any disclosure, publication, or revelatior

6. I understand that the United States Governmer limited to, application for a court order prohibiting d

7. I understand that all classified information to w remain the property of, or under the control of the official or final ruling of a court of law. I agree that for which I am responsible because of such a Government; (b) upon the conclusion of my empl security clearance or that provided me access t relationship that requires access to classified infor a violation of sections 793 and/or 1924, title 18, Un

8. Unless and until I am released in writing by a conditions and obligations imposed upon me by t and at all times thereafter.

9. Each provision of this Agreement is severable. provisions of this Agreement shall remain in full for

10. These provisions are consistent with and do liabilities created by existing statute or Executive reporting to an Inspector General of a violation of authority, or a substantial and specific danger to requirements, obligations, rights, sanctions, and incorporated into this agreement and are controlling

NSN 7540-01-280-5499
Previous edition not usable.

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud , abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community. and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001 , section 2001 .80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT
SIGNATURE / DATE	SIGNATURE / DATE
NAME AND ADDRESS (Type or print)	NAME AND ADDRESS (Type or print)

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

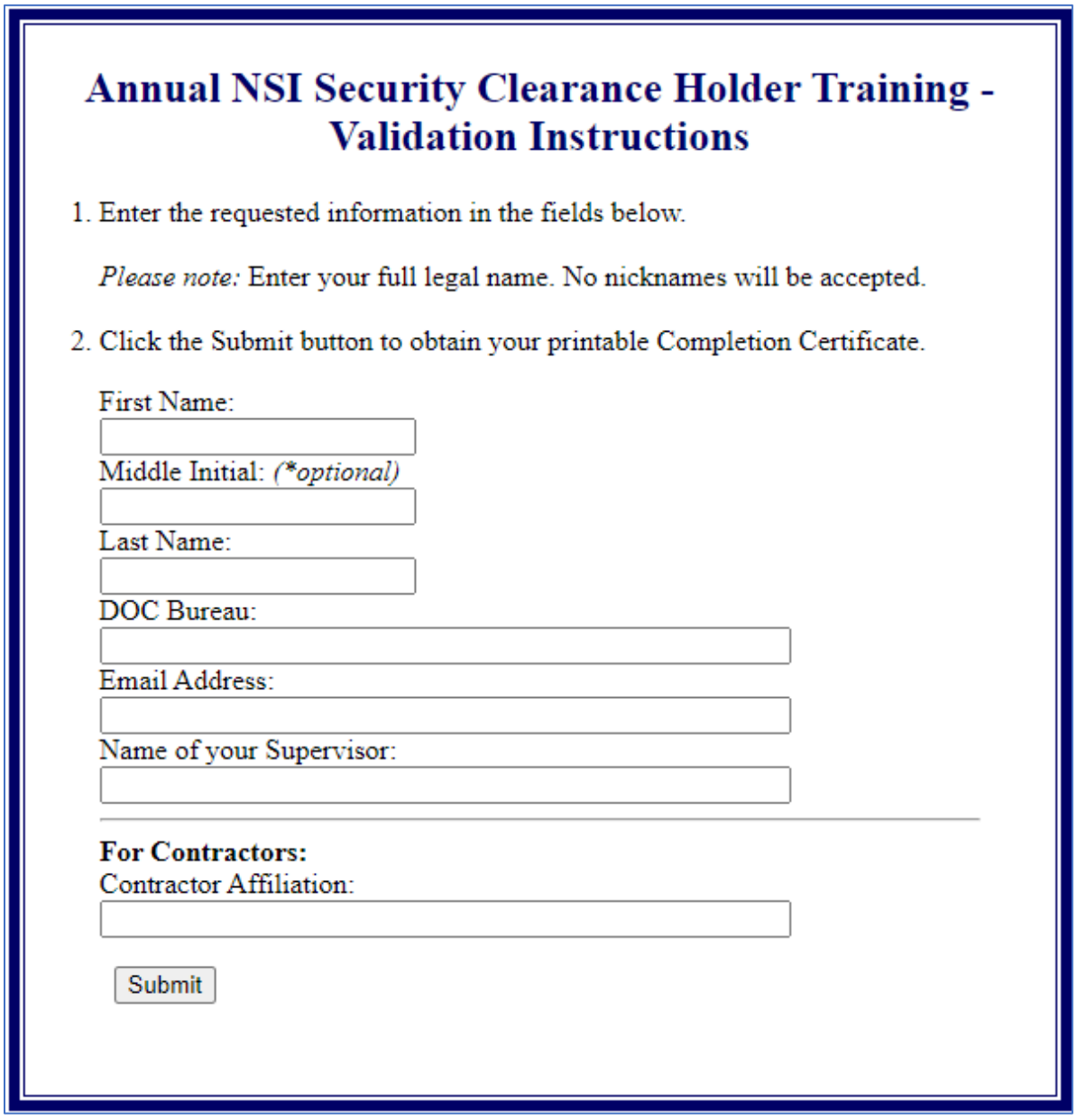
NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

STANDARD FORM 312 BACK (Rev. 7-2013)

Attachment 2: SF-312 Classified Information Nondisclosure Agreement Instructions

1. Download SF-312 Classified Information Nondisclosure Agreement
2. Top - Type or Print your name. First and Last name at a minimum.
3. SSN - Only place the last four digits of your Social Security Number.
    - Example: 000-00-1234 (The digital version requires nine digits)
4. Organization – Department FAC you support and physical address to the FAC. Do not include your home or personal addresses.
    - Example: Commerce Data Advisory Council – 1401 Constitution Ave NW, Washington, DC 20230
5. Signature – Digital
    - If digitally signing with your Department-issued PIV certificate, no witness is required.
6. Signature – Ink
    - Signature must be witnessed if ink signing. The witness may do this in person or remotely using agency approved communication tools/software such as Skype, WebEx, or Microsoft Teams.
7. Witness Block
    - Witness MUST be a Federal Employee.
    - Must place First name, Last name AND federal work address below signature.
8. Date Boxes – Ensure the dates are the same. The witness's signature validates that your signature was witnessed on that date.
9. Acceptance Box – LEAVE BLANK
10. Security Debriefing Acknowledgment – LEAVE BLANK
11. Contact OSY at: osy_infosec@doc.gov for further instructions on how to securely submit your SF-312.
    - Personally Identifiable Information must be sent via secure means either through Kiteworks or by password protecting the document and sending the password under separate cover.

Attachment 3: Web-based training Validation Instructions



Annual NSI Security Clearance Holder Training - Validation Instructions

1. Enter the requested information in the fields below.

   Please note: Enter your full legal name. No nicknames will be accepted.

2. Click the Submit button to obtain your printable Completion Certificate.

First Name:

Middle Initial: *(*optional)*

Last Name:

DOC Bureau:

Email Address:

Name of your Supervisor:

For Contractors:

Contractor Affiliation:

Submit

Attachment 4: Web-based training Certificate of Completion

Certificate of Completion

I am Secure

isecure@doc.gov
Supervisor: John Q Supervisor

completed the

Annual NSI Security Clearance Holder Training

on

Thursday, October 27, 2022

To obtain credit for completing this course, please provide a signed copy of this completion certificate by emailing OSY_Infosec@doc.gov.

Digitally signed by [redacted]
Date: 2022.10.27 08:10:56 -04'00'

Your Signature: _____

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA