MEMORANDUM FOR: Distribution

SUBJECT: National Operations Security Program


As set forth in National Security Presidential Memorandum (NSPM) -28 (Ref), the National Operations Security (OPSEC) Program (NOP) supports the establishment, implementation, and standardization of stakeholder OPSEC programs across the Executive Branch of the U.S. Government (USG) and, as appropriate, beyond to trusted partners.

In short, NSPM-28 requires all Executive Branch departments and agencies implement OPSEC capabilities that identify and protect their most critical assets, identify and mitigate vulnerabilities, consider foreign adversarial threat in their organizational risk management activities, and apply sufficient threat mitigation practices to counter the threat. NOP requirements are set forth in NSPM-28.

NCSC’s Enterprise Threat-Mitigation Directorate (ETD) will execute the roles and responsibilities of the NOP Program Office, as described in NSPM-28 and will support department and agency implementation of OPSEC programs. NCSC/ETD will provide additional guidance, work with all Executive Branch departments and agencies to develop their programs, and will provide program development, training, and awareness materials.

The attachment identifies program implementation tools and access to Interagency OPSEC Support Staff (IOSS) training registration. Note that the IOSS Operations Security Analysis and Operations Security Manager courses will remain available through calendar year 2022 to support program establishment throughout the USG. We will share newly developed professional and awareness opportunities as they become available.

If you have any questions regarding the NOP or professionalization and awareness resources please contact NCSC/ETD at ncsc_feds@dni.gov.

Michael J. Orlando
Acting Director

UNCLASSIFIED
SUBJECT: National Operations Security Program

Attachment:
National OPSEC Program Resources
SUBJECT: National Operations Security Program

Distribution:
Secretary of Agriculture, Department of Agriculture
Secretary of Commerce, Department of Commerce
Secretary of Defense, Department of Defense
Secretary of Education, Department of Education
Secretary of Energy, Department of Energy
Secretary of Health and Human Services, Department of Health and Human Services
Secretary of Homeland Security, Department of Homeland Security
Secretary of Housing and Urban Development, Department of Housing and Urban Development
Secretary of the Interior, Department of the Interior
Attorney General, Department of Justice
Secretary of Labor, Department of Labor
Secretary of State, Department of State
Secretary of Transportation, Department of Transportation
Secretary of the Treasury, Department of the Treasury
Secretary of Veterans Affairs, Department of Veterans Affairs
Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, Office of Intelligence and Counterintelligence, Department of Energy
Under Secretary, Intelligence and Analysis, Department of Homeland Security
Assistant Secretary, Bureau of Intelligence and Research, Department of State
Assistant Secretary, Intelligence and Analysis, Department of the Treasury
Chief of Intelligence/Senior Officer (SOIC), Drug Enforcement Administration
Executive Assistant Director, Intelligence Branch, Federal Bureau of Investigation
Director, National Geospatial-Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Deputy Chief of Staff - G2, Headquarters, United States Army
Director of Naval Intelligence, United States Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force
Director of Intelligence, Headquarters, United States Marine Corps
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard
Director, United States Secret Service
Under Secretary of Defense for Intelligence, Department of Defense
Chairman, Joint Chiefs of Staff
Secretary of the Air Force, United States Air Force
Secretary of the Army, United States Army
Secretary of the Navy, United States Navy
Commandant of the Marine Corps, United States Marine Corps
Chief, National Guard Bureau
Director, Defense Information Systems Agency Distribution, cont'd:
Director, Defense Logistics Agency
Director, Missile Defense Agency
Inspector General, Department of Defense
SUBJECT: National Operations Security Program

Director, Defense Security Service
Director, Defense Advanced Research Projects Activity
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Services
Director, Bureau of Alcohol, Tobacco, Firearms and Explosives
Director, Broadcasting Board of Governors
Administrator, Drug Enforcement Administration
Administrator, Environmental Protection Agency
Administrator, Equal Employment Opportunity Commission
Chairman, Federal Reserve Board, Federal Reserve System
Chairman, Federal Communications Commission
Chairman, Federal Maritime Commission
Chairman, Federal Trade Commission
Administrator, General Services Administration
Director, Information Security Oversight Office
Chairman, International Trade Commission
Director, Office of Management and Budget
Administrator, National Aeronautics and Space Administration
Archivist, National Archives and Records Administration
Director, National Science Foundation
Chairman, Nuclear Regulatory Commission
Director, Office of Government Ethics
Director, United States Peace Corps
Director, Office of Personnel Management
Chief Postal Inspector, United States Postal Inspection Service
Chairman, Securities and Exchange Commission
Director, Office of Science and Technology Policy
Director, Selective Service System
Administrator, Small Business Administration
Commissioner, Social Security Administration
Administrator, United States Agency for International Development
Commissioner, United States Customs and Border Protection
United States Trade Representative
Director, White House Office of the National Drug Control Policy
Postmaster General, United States Postal Service
Director, Executive Office of the President, Office of Administration
Chairman, National Labor Relations Board
SUBJECT: National Operations Security Program

Attachment 1: National OPSEC Program Resources

Interagency OPSEC Support Staff (IOSS), https://www.iad.gov/ioss: this website requires registration and provides training and resources for the entire USG.

Virtual Instructor-led Training

- OPSEC 2380 Analysis Course
- OPSEC 2390 Program Manager Course

Note: These virtual instructor-led courses will sunset in December 2022. At that time, additional materials will be provided to ensure the community has the necessary knowledge, skills, and abilities to effectively implement National OPSEC Program requirements and minimum standards. That body of material, which includes eLearning courses, job aids, and other resources, will serve as the foundational training for OPSEC program practitioners in the Executive Branch departments and agencies. The NOP Office will provide additional information on alternative learning platforms and training capabilities as they become available.

In the interim, the NOP Office recommends the following IOSS materials for OPSEC Program Managers and other federal partner security practitioners for general program awareness and implementation guidance:

Program Implementation Job Aids provided via https://www.iad.gov/ioss: (Awareness Products<Practitioners Toolbox)

- OPSEC Program Managers Handbook. This handbook is designed to assist the OPSEC manager in developing a formal program. This publication is for guidance only and is not to be used as the sole content of any OPSEC program or plan.

- Appointment Letter for OPSEC Officer. One example of an OPSEC officer appointment letter used by organizations to officially designate an individual as the command/organization OPSEC Officer, Program Manager, or Coordinator.

- OPSEC Program Checklist. This checklist enhances the Program Manager’s ability to track and ensure all areas of a new or updated program have been addressed. This list should identify all of the necessary documentation, timelines, and personnel issues (to include training requirements) and associated operational support issues. This is a guide and must be tailored to meet individual department/agency needs.

- OPSEC Survey Interview. The OPSEC Survey Interview is a basic guide to evaluate personnel knowledge of OPSEC as it applies to their current duties, OPSEC in relation to the organization to which they are assigned, and their overall knowledge and understanding of OPSEC principles. Questions concerning specific events or missions
SUBJECT: National Operations Security Program

should be intermingled throughout the interview or agreed upon by the team prior to
beginning the interview process.

- OPSEC Survey Interview Sheet. The OPSEC Interview Sheet is used by the person
conducting the interview as a guide and to record their observations or concerns noted
during the interview process.

- Critical Information Policy. This is a guidance document designed to disseminate the
department/agency Critical Information List to all personnel. It may be used to solicit
Critical Information to be included in an organization-wide list. It enforces the
department/agency head’s instructions concerning the handling and protection of the
information indicated.

- OPSEC Program Plan. The OPSEC Program Plan outlines how OPSEC will be
employed throughout an organization, the responsibilities of the OPSEC Program
Manager, the role of the OPSEC working group members, and guidance for each step of
the OPSEC program. Specific guidance pertaining to program organization and all
functional areas are addressed in this document.

IOSS OPSEC Computer-Based Training (CBT) Course Catalog (https://www.iad.gov/iooss)

- Cyber OPSEC Awareness CBT Course Description: CYBER OPSEC Awareness CBT
focuses on understanding cyber threats and how to incorporate OPSEC practices to
protect cyber-related infrastructure and activities.

- Critical Infrastructure OPSEC Course, “What’s in it for me?” CBT Course Description:
An OPSEC and Critical Infrastructure and Key Resources (CIKR) computer-based
training product. This training focuses on OPSEC as it relates to the following four
CIKR sectors: Financial; Emergency Services; Energy, and; Transportation. Scenarios
for each sector focus on human, physical, and cyber vulnerabilities and countermeasures
for each. This training is designed for people who support homeland security efforts. An
introduction to OPSEC is available for those who have limited training in operations
security.

- New Faces of Threat CBT: This training is intended for OPSEC practitioners. The
current technological landscape is vast; advancements seem to happen within the blink of
an eye. This expansive cyber terrain has cultivated a dangerous cyber threat. The
adversary’s symbiotic relationship with technology allows them to exploit it for their own
gains. To stay ahead of the threat and remain secure, OPSEC practitioners must prepare.
This requires a solid understanding of the vulnerabilities hidden within new technology,
knowledge of the possibilities for exploitation inherent in the cyber world, and access to
the best countermeasures available.
SUBJECT: National Operations Security Program

- OPSEC University CBT Course Description: Welcome to OPSEC University, an interactive, informative, and fun way to learn about Operations Security, aka OPSEC! This dynamic, computer-based awareness tool is divided into three parts: “OPSEC 101” for beginners; the annual “Refresher” for returning students, and; a Resources section that contains draft documents to help you further develop your OPSEC program. In just a couple of hours you will work your way through a variety of scenarios, test the knowledge you have gained through “quiz show” games, and reinforce it with a poster that you can print right from the training software provided via https://www.iad.gov/ioss.

- Integrating OPSEC Into Contracts CBT Course Description: This tutorial focuses on applying the OPSEC process to protect U.S. critical information during the contracting cycle. It begins with a short OPSEC overview, then walks acquisition personnel through their individual roles and responsibilities. The disk also includes a Tools section where contracting officers, program managers, etc., may access forms and guidance to help them build a program and integrate OPSEC into their contracts.