Does ODNI have a System of Records Notice (SORN) that covers the information requested in SEAD 3?

ODNI is not the statutory "owner" of personnel security records for the entire government, and will not, therefore establish a U.S. Government-wide SORN. Because the matters reported are subject to investigation and adjudication by individual employing security elements D/As should already have a SORN and routine use clause covering collection and sharing of such information.

Will additional monetary resources be provided to D/As to implement SEAD 3?

Additional resources will not be provided to implement SEAD 3. Various Executive Orders requiring D/A heads to establish effective security programs to ensure that employment and continued employment of individuals in D/A are longstanding and consistent with the interests of national security. In 2014, President Obama approved recommendations to expand and clarify reporting requirements. Please refer to the 120-Day Report-Suitability and Security Process Review Report to the President dated February 2014. D/As are encouraged to project necessary budgetary requirements for implementation, sustainment and maintenance of their personnel security programs.

Will D/As be assessed for effectiveness compliance?

The ODNI established the Security Executive Agent National Assessment Program (SNAP) to conduct oversight of personnel security programs. Assessments will evaluate compliance in SEAD 3 implementation, measure program effectiveness, gather metrics, trends and lessons learned. Understanding D/As require time to fully implement SEAD 3, SNAP assessments will be coordinated in advance.

Do D/As have a legal basis to disapprove unofficial travel? Can D/As develop a list of pre-approved countries?

D/As have the authority to disapprove unofficial travel in the interest of national security when the D/A determines that such travel presents an unacceptable national security risk and the physical safety and security of covered individuals or classified information cannot be reasonably ensured. D/As may develop a list of pre-approved countries.

What is the requirement for D/As to train the workforce?

D/As are responsible for providing training, to include ensuring awareness of individual reporting obligations during employee orientation, security indoctrination, and annual refresher training.

How does SEAD 3 apply to employees stationed overseas?

SEAD 3 applies to all covered individuals with a security clearance or who occupy a sensitive position, regardless of location or D/A. It is understood that mission requirements vary, so SEAD 3 provides flexibility. D/As have the ability to identify conditions, consistent with national security, under which reporting and approval of foreign travel is not required.

Produced by the Office of the Director of National Intelligence

For Use by U.S. Government Civilian, Military and Contractor Personnel.
May 17, 2017 • Version 1

FREQUENTLY ASKED QUESTIONS
FOR DEPARTMENTS AND AGENCIES

SEAD 3

SECURITY EXECUTIVE AGENT DIRECTIVE 3:

Reporting Requirements for Personnel
with Access to Classified Information
or Who Hold a Sensitive Position

When is SEAD 3 implementation required?

Implementation of SEAD 3 is 12 June 2017.

What if my Department/Agency (D/A) will not make the 12 June implementation date?

Each D/A is expected to start implementing SEAD 3 by the effective date. As with any rollout, we do not expect full operating capability on the effective date. If an extension is required, the D/A head should submit a written justification to the National Counterintelligence and Security Center, Special Security Directorate, identifying the proposed plans and date to meet the requirement.

How would D/As that do not have automated database systems maintain and analyze the required information by the 12 June 2017 effective date?

When automation by 12 June 2017 is not practicable, reported information may be received, reviewed, and retained in any secure format that meets your D/A requirements. Information can be administered as hardcopy, e-mail, spreadsheet, or by using other methods that work best for the D/A.

Would you share analytic best practices or lessons learned from other D/As currently implementing SEAD 3-type requirements?

During this SEAD 3 Forum, representatives of large and small Executive Branch D/As will share their best practices and lessons learned. Additionally, the Office of the Director for National Intelligence (ODNI) created a tool kit and resources for your use; available at DNI.Gov/NCSC/KnowtheRiskTools.

Is there a whole-of-government reporting system available for SEAD 3 implementation?

Traditionally, the Executive Branch D/As have established specific reporting requirements and programs to capture this data. The Department of Defense, with the Performance Accountability Council's endorsement, is creating an electronic reporting capability for optional use by D/As in the near future.

Who reviews guidance for unique situations, and what do we do with the information we collect?

D/As are expected to determine internal procedures and follow legal, information management, and privacy requirements for the receipt, review, and retention of reported information.

Are there official thresholds for what should be reported?

Thresholds for reporting will vary by D/A, along with consideration of the circumstances surrounding the events. In general, D/As should determine the potential risk to national security equities.

Who handles discipline for those who fail to comply with self-reporting requirements?

D/As are responsible for handling disciplinary actions for individuals that do not report. Thresholds for failure to report will vary by D/A, along with consideration of the circumstances surrounding the events. In general, D/As should determine the impact to national security equities.

What resources are available for use to assist D/As in implementing SEAD 3?

D/As should consult with agency subject matter experts (i.e. security, counterintelligence, insider threat, legal, human resources, privacy and civil liberties) to implement SEAD 3.

For government labor union personnel, how should legal notification be made and challenges to this policy be handled? Has this issue been addressed with the Office of Personnel Management (OPM)?

OPM was included in the interagency review of SEAD 3. D/As should utilize existing union notification procedures to inform union members of the requirements of SEAD 3. Personnel security reporting requirements are considered internal security practices within management's right to impose under the Federal Service Labor/Management Relations Statute, 5 USC § 7106.

How should government employees with dual citizenship in sensitive positions be handled for these reporting requirements?

These individuals are to be handled in the same manner as non-dual citizens and those with a security clearance who have foreign activities, foreign contacts, and travel. If a reportable event occurs, it should be reported. Please note, for dual citizens, most events that need to be reported would have already been addressed. Only new events since the last investigation would need to be reported. Those individuals who obtained dual citizenship after their last investigation would need to report this as a new event.

How do cleared academia professionals, laboratory personnel, and consultants comply with SEAD 3's reporting requirements?

These individuals should continue to be included in existing reporting processes. Sponsoring D/As are encouraged to reach out to the individuals within these specialized programs to inform them about reporting requirements and how to self-report.

Where can I seek additional information and guidance on SEAD 3?

Consult your local security office for information and guidance.

How should D/As handle and store reported information?

In general, D/As must administer the receipt and retention of reported information in accordance with all applicable law and policy, including statutes, Executive Orders, regulations, and agency internal policies. Where privacy matters are implicated, D/As must be compliant with Privacy Act requirements and ensure that sensitive reporting information is properly safeguarded. All D/As must coordinate with the offices of General Counsel, Privacy and Civil Liberties and Records Management.