

REPORTING REQUIREMENTS

INSIDER THREAT AND
ADVERSE INFORMATION

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

SISR Ehren Thompson





Agenda

- Security Executive Agent Directive (SEAD) 3
- SEAD 3 and Adverse Information Reporting Requirements
- Security Practice Procedures (SPP) & Industrial Security Letter (ISL) 2021-02
- Insider Threat Program and Reporting Requirements
- Security Education Tools and Best Practices

Security Executive Agent Directive (SEAD) 3



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

Purpose: This Security Executive Agent Directive establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.



Foundations of SEAD 3

Establishes reporting requirements for all covered individuals who have access to classified information or who hold a sensitive position.

Covered individuals have a special & continuing security obligation and responsibility for recognizing, avoiding, and reporting personal behaviors of a potential security, counterintelligence, and/or insider threat concern.

Individuals must alert their FSO should they become aware of certain activities. The FSO must work with the ITPSO to mitigate these events.



Reportable Actions by Others

An unwillingness to comply with rules, regulations, or security requirements

Unexplained affluence or excessive indebtedness

Alcohol abuse

Illegal use or misuse of drugs or drug activity

Apparent or suspected mental health issues that may impact the individual's ability to protect classified information or information prohibited by law from disclosure

Criminal conduct

Misuse of U.S. Government property or information systems



Reportable Actions by All

Changes in Personal Status

Foreign Travel

Foreign Contact

Loss or Compromise of Information

Financial Problems

Arrests

Psychological or Substance Abuse Counseling

Reportable Actions: Secret or Confidential Clearance



Foreign Activities

- Application for and receipt of foreign citizenship
- Application for, possession, or use of a foreign passport or identity card for travel

Other Activities

- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified or proprietary information
- Media contacts, other than for official purposes
- Arrests
- Bankruptcy or over 120 days delinquency on any debt
- Alcohol or drug-related treatment



Reportable Actions: Top Secret Clearance

Foreign Activities

- Direct involvement in foreign business
- Foreign bank accounts
- Ownership of foreign property
- Voting in a foreign election
- Adoption of non-U.S. citizen children

Other Activities

- Financial anomalies (wage garnishments)
- Foreign national roommate(s)
- Cohabitant(s)
- Marriage



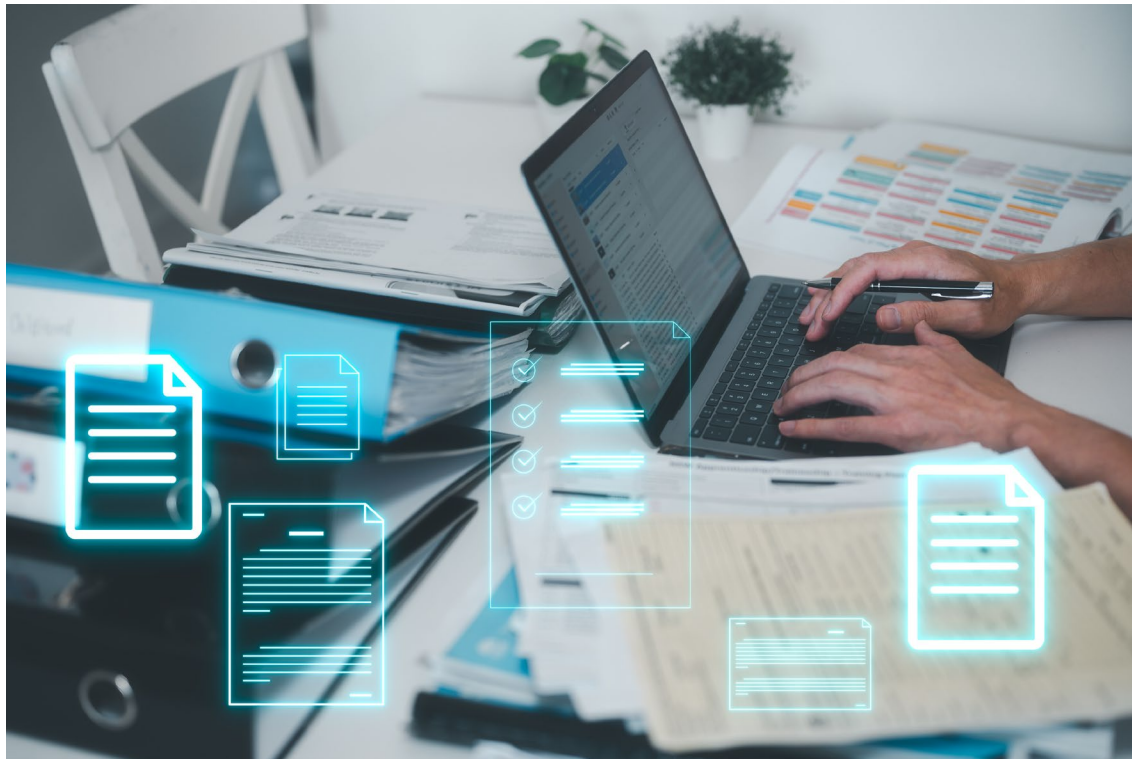
Industrial Security Letter 2021-02

- ISL 2021-02 provides clarification and guidance on adverse information reporting and SEAD 3 reporting requirements.
- Some of the changes are intended to better align with national policy for the protection of Classified National Security Information, some are to address changes in law or regulations, and some are to enhance the protection of classified material that contractors access or possess.





Standard Processes and Procedures (SPP)



The Contractor's SPP must establish the necessary processes and procedures to inform their cleared contractor personnel on reporting requirements related to SEAD 3 and the requirements for adverse information reporting as directed by the NISPOM rule at section 117.8(c)(1).



Insider Threat Program Requirements

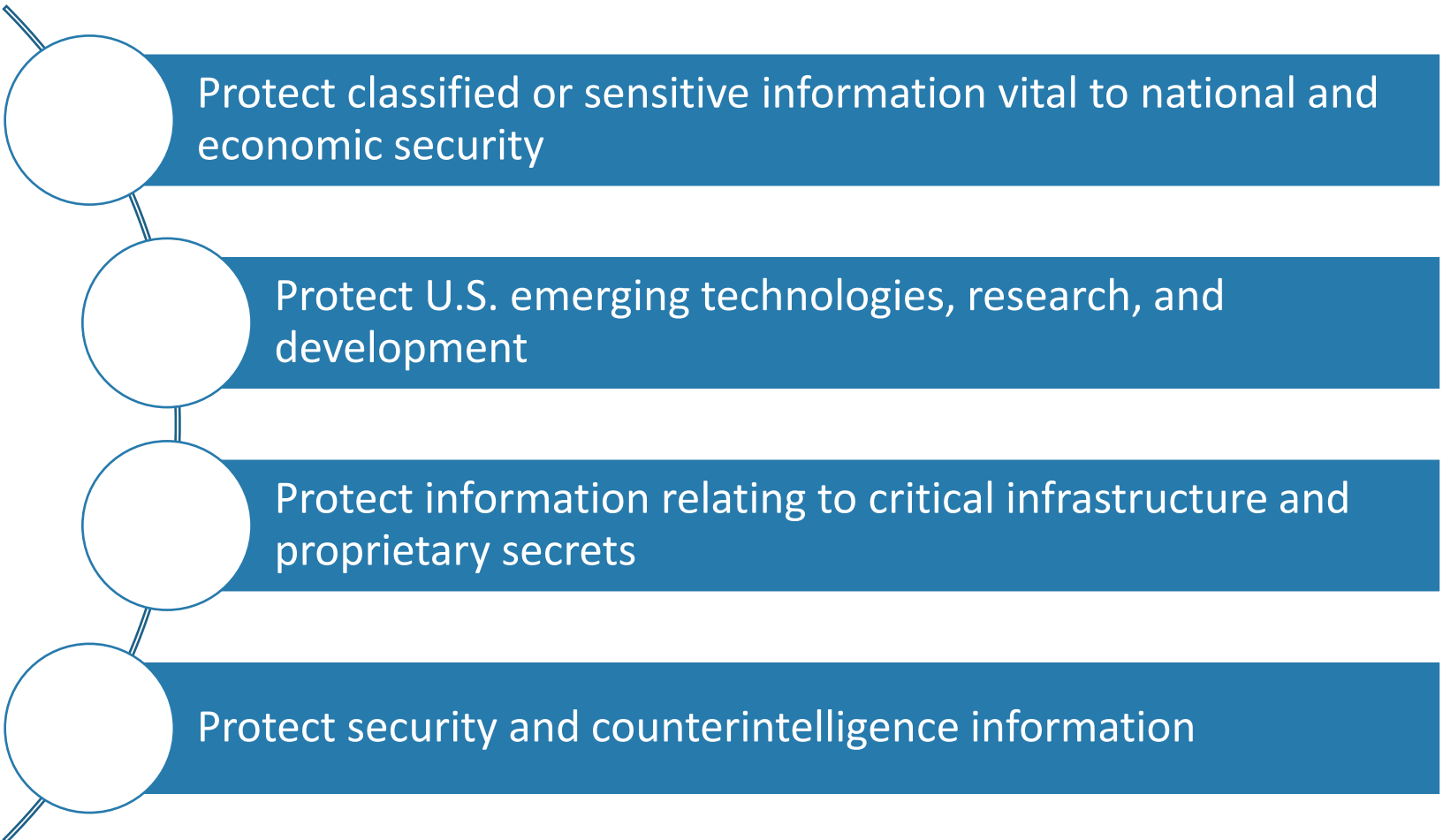
Contractor Insider Threat Programs MUST:

- Appoint an Insider Threat Program Senior Official (ITPSO)
- Provide initial and refresher insider threat training for cleared employees
- Place necessary controls on classified information systems
- Be capable of gathering relevant information across a contractor facility
- Leverage procedures to identify and report information indicative of a potential or actual insider threat
- Detect, deter, and mitigate the risk of insider threat





Why Report?

A vertical diagram consisting of four white circles connected by a thin line. Each circle is positioned to the left of a blue rectangular box containing white text. The circles have a small line extending from the top-left and bottom-left, giving them a 3D appearance.

Protect classified or sensitive information vital to national and economic security

Protect U.S. emerging technologies, research, and development

Protect information relating to critical infrastructure and proprietary secrets

Protect security and counterintelligence information



Security Education

Provide initial and annual security briefings to employees

Establish an insider threat program

Conduct regularly occurring insider threat working group meetings

Facilitate active communication with the insider threat working group

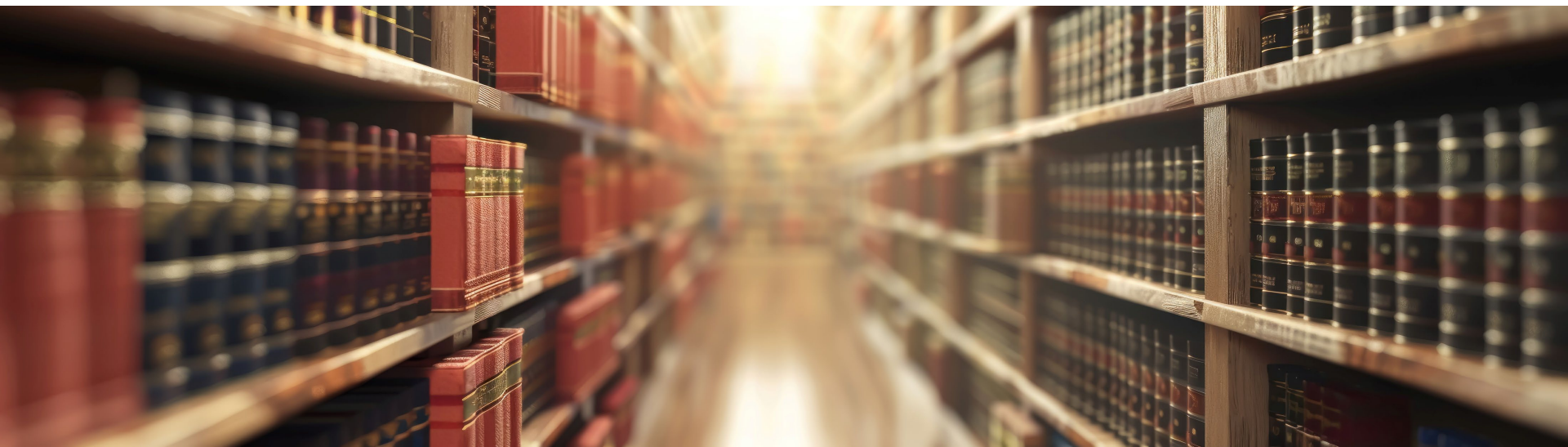
Encourage adverse information reporting

Report suspicious contacts



References

- [Insider Threat Toolkit](#)
- [ISL 2021-02](#)
- [SEAD 3 Reporting Requirements](#)





Contact Us

NAESOC Knowledge Center

1(888) 282-7682, option 7 (NAESOC)

NAESOC General Mailbox

dcsa.naesoc.generalmailbox@mail.mil