

In 2017 the Director of National Intelligence (ODNI) acting in its capacity as the Security Executive Agent (SecEA) announced a third revision to the Security Executive Agent Directive (SEAD), now known as SEAD 3. Although announced last year, some agencies have only achieved full compliance with SEAD 3 within the last few months.

Aiming to reduce insider threats, the directive dramatically expands reporting responsibilities for public contractors who deal with sensitive or classified information, whether their personnel are cleared individuals or merely occupy "sensitive positions". A major impact of SEAD 3 is that non-cleared individuals may have to file reports before and after traveling to any foreign country.

### OVERVIEW OF NEW REQUIREMENTS

Prior to SEAD 3, reporting duties for cleared personnel were mainly defined by Title 10 of the Code of Federal Regulations (CFR), which require a Department or Agency (D/A) to be notified under circumstances, such as

- Arrests, charges or detentions
- Travel to a foreign country requiring a non-US passport
- Foreign national contacts
- A change in marital status

While this list is non-comprehensive, it generally reflects the level of scrutiny that has been directed towards individuals with a security clearance. Employers have been responsible for monitoring their own personnel, and reportable events have been limited in scope.

Under SEAD 3, cleared individuals are now required to file self-reports for a wider range of events, including:

- "Continuing association" with any foreign national which, according to the ODNI, can extend to social media contacts.
- Adoption of non-U.S citizen children
- New cohabitants (such as room, housemates or significant others)
- Treatment for a drug or alcohol-related issues
- Any travel to a foreign country with full itinerary

SEAD 3 creates a responsibility to report other cleared individuals who are suspected to meet these criteria without filing a report. Significantly, the new requirements extend to non-cleared individuals who occupy a "sensitive position," defined broadly as:

*"Any position within or in support of an agency in which the occupant could bring about, by virtue of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor."*

In theory, this could include any number of personnel working alongside cleared individuals, including janitorial staff, office assistants, vendors, etc. The ODNI has left discretion to agencies in defining the scope of this role and advises contractors to consult their D/A for clarification.





## NEW TRAVEL REQUIREMENTS

Significantly, SEAD 3 has broad stipulations about non-official foreign travel. Cleared personnel and those in sensitive positions must submit a full itinerary of their trips ahead of time, including

- **Route and destinations**
- **Dates of travel**
- **Mode of travel & identification of carrier**
- **The names of any traveling companions, regardless of relation**


If any alterations occur during the trip, or any “unplanned contact” with foreign nationals, these must be reported within five days of return.

## MOVING FORWARD

Obviously, the strictness of SecEA’s new standards exacts a significantly larger report-handling load from both individuals and contractors. For this reason, the Nuclear Regulatory Commission (NRC) requested a year-long extension from the ODNI before compliance went into effect.

This year, when advised by personnel that the new requirements were “too burdensome,” the NRC frankly replied, “we agree.” It went on to add, “We may have some methods to now address the issue.”

As legislation continues to comprehensively address the need for tightened standards in America’s security community, it is incumbent on contractors and agencies to utilize security compliance tools and resources to meet their expanded reporting responsibilities.



MathCraft Security Technologies offers a robust product line of NISPOM-compliant security applications for cleared contracts and enterprises. Our solutions are carefully engineered to improve security processes, giving Facility Security Officers (FSOs) and employees the comprehensive tools that they need to manage data, monitor visitors, and automate workflows. For ultimate convenience, they are also available on-premises or via the cloud.