Biennial Report to Congress on Improving Industrial Security

U.S. Department of Defense

February 2015

The estimated cost of this report or study for the Department of Defense is approximately $13,606 for the 2015 Fiscal Year. This includes $2,273 in expenses and $11,333 in DoD labor.
Generated on 2015Mar12 RefID: 0-8FE5449

Biennial Report to Congress on Improving Industrial Security

This report complies with Section 845 of the National Defense Authorization Act (NDAA) for fiscal year 2009 (Public Law 110-417), which requires the Secretary of Defense to report biennially to the congressional defense committees on expenditures and activities of the Department of Defense (DoD) in carrying out the requirements of this section (i.e., Defense Industrial Security). Unless otherwise stated, all information contained in this report covers fiscal year (FY) 2013 through 2014.

Topic I: The workforce responsible for carrying out the requirements of this section, including the number and experience of such workforce; training in the performance of industrial security functions; performance metrics; and resulting assessment of overall quality.

The below chart reflects the Defense Security Service (DSS) planned workforce for FY13 and FY14 to provide direct support to the oversight and administration of the National Industrial Security Program (NISP) and shows actual manning against the planned billets.

Defense Security Service	FY13 - AUTH	FY13 - ACTUAL	FY14 - AUTH	FY14 - ACTUAL
Industrial Security Field Operations Directorate	407	407	406	369
Industrial Policy and Programs Directorate	61	61	61	61
Personnel Security Management Office for Industry	26	36	37	37
Counterintelligence Directorate	134	134	142	143
Center for Development of Security Excellence	72	72	72	83
TOTALS	710	710	718	692

The Industrial Security Field Operations (IO) Directorate is the primary operational element of DSS that has responsibility for overseeing the protection of classified information by cleared companies across the United States. IO is comprised of industrial security representatives (ISRs), who are general security specialists, as well as information systems security professionals (ISSPs), who are technical experts certified in accordance with DoD and national standards. ISRs perform periodic security reviews and vulnerability assessments, and monitor cleared companies' compliance with the NISP. ISSPs oversee, certify, and recommend accreditation of cleared industry information systems to process classified information. The

ISSPs and ISRs also support the U.S. Cyber Command's cyber readiness inspection mission by evaluating cleared industry Secret Internet Protocol Router Network (SIPRNet) nodes. The IO Directorate includes a headquarters element that oversees field personnel, processes and grants requests for facility clearances (FCLs), and monitors conditions affecting those FCLs.

The Personnel Security Management Office for Industry (PSMO-I) is responsible for the management and oversight of approximately 940,000 contractors with clearances. Functions include review and submission of 220,000 Electronic Questionnaires or Investigations Processing (e-QIP) and 80,000 interim clearance determinations per year. Other functions include validating and storing contractor Non-Disclosure Agreements (SF-312s), conducting oversight and continuous evaluation of contractor clearances to ensure the timely submission of Periodic Reinvestigations and triaging incident reports, ensuring Industry unique requirements are programmed in personnel security information technology systems, implementing new policy and processes, and serving as customer service liaison.

The Industrial Policy and Programs (IP) Directorate is an organizational element of DSS that adjudicates foreign ownership, control or influence (FOCI) issues, monitors compliance by cleared companies under FOCI with FOCI mitigation agreements, administers international programs, establishes NATO control points in cleared industry, conducts NATO control point inspections, and provides industrial and personnel security policy guidance to cleared industry. Part of the IP Directorate's FOCI mission includes providing DSS input to the DoD lead for the Committee on Foreign Investment in the United States (CFIUS) on all covered CFIUS transactions when the transactions involve cleared companies that will be under the FOCI mitigation requirements of the National Industrial Security Program Operating Manual (NISPOM).

The Counterintelligence (CI) Directorate identifies known or suspected collectors involved in illicit attempts to obtain classified or U.S. Government-controlled technology and information resident in cleared companies, and articulates the CI threat to cleared industry. The CI Directorate refers incidents indicating possible attempts to illicitly obtain technology, or to compromise cleared industry personnel, to national CI and law enforcement agencies for investigative follow-up or operational exploitation. The CI Directorate addresses threats to cleared industry that manifest through all venues, to include technical, human, and information system means.

The Center for Development of Security Excellence (CDSE) is the premier provider of security education, training, and certification for the Department of Defense and cleared industry. CDSE provides development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing our nation's security challenges.

DSS is constantly evaluating its training and assessing the quality of its workforce and is confident it has a high quality, high performing workforce. To further the ability of the DSS workforce to perform its oversight mission and enhance industrial security, DSS is making key investments in technology. The technology under development would automate manual processing, improve analysis, facilitate data sharing across the Department, and promote access to secure data.

All new ISRs assigned to DSS participate in a formal mentoring program with more experienced personnel. They participate in formal training divided into two programs of instruction: Fundamentals of Industrial Security and NISP Information Assurance Fundamentals. The Fundamentals of Industrial Security Level 1 (FISL 1) course offers an interactive, blended learning format consisting of eLearning, mentoring, structured field activities (some of which are evaluated by instructors), on-the-job training, and formal assessments. The course provides new ISRs a baseline understanding of the requirements and core responsibilities of the DSS industrial security mission. It focuses on teaching industrial security requirements and internal DSS processes and procedures to prepare ISRs to perform independently in the field.

Upon completion of FISL 1, ISRs complete the Fundamentals of Industrial Security Level 2 (FISL 2) course. FISL 2 is an in-class, instructor-led course consisting of directed discussion, practical exercises based on real work examples and assessments. The course is designed to prepare the ISRs to conduct security assessments, surveys and other actions. Specialized training in counterintelligence fundamentals, information systems, business structures and other areas is available for individuals serving in those positions.

ISSPs assigned to DSS complete NISP Information Assurance Fundamentals, an interactive, blended learning format course consisting of eLearning, mentoring, structured field activities (some of which are evaluated by instructors), on-the-job training, and formal assessments. The course provides ISSPs with a baseline understanding of the requirements and core responsibilities of the DSS industrial security mission. It focuses on teaching fundamentals of information assurance, cybersecurity, industrial security requirements, and internal DSS processes and procedures to prepare the ISSPs to perform independently in the field.

All DSS ISSPs must also complete annual continuing learning credits to maintain their required certification (e.g., Certified Information Systems Security Professional). Additionally, selected ISSPs are trained and certified by the Defense Information Systems Agency (DISA) to conduct cyber readiness inspections. This advanced training includes hands-on instruction with cyber professionals using DoD-approved tools.

CI special agents are typically hired into DSS with extensive backgrounds in CI and/or law enforcement, and have typically served in credentialed CI or federal law enforcement positions within the military services or other U.S. Government agencies. Additional training is provided to CI special agents and headquarters intelligence analysts through the Joint Counterintelligence Training Academy or other intelligence community training sources.

DSS offers 53 instructor-led and eLearning courses related to industrial security, cybersecurity, and CI awareness. During the reporting period, DSS personnel with Industrial Security Program oversight responsibilities participated in and completed 9,077 training courses and 93 achieved the Industrial Security Oversight Certification. Also, industry personnel participated in and completed 75,189 training courses, and 5 personnel achieved the Industrial Security Oversight Certification. Detailed information on these training courses is contained in Appendix A.

CDSE introduced a new curriculum of 17 graduate-level courses in FY12 and FY13, designed to prepare DoD security specialists for leadership positions and responsibilities. During FY13 and FY14, DSS personnel with Industrial Security Program responsibilities completed 36 graduate courses for 108 graduate credit hours. An additional 207 graduate courses (621 graduate credit hours) were completed by security professionals working for other DoD agencies, military services and other Federal agencies.

DSS established metrics to evaluate its performance and resource efficiency in the oversight and administration of the NISP, and to troubleshoot problem areas. To gather this information, DSS developed a system of data collections across the agency to compile the information. The following are examples of the metrics DSS gathers to monitor its performance. All information is current as of September 30, 2014. (Note: "days" refers to calendar days.)

- In FY13, DSS received 2,885 FCL sponsorship requests.[1] Of these, DSS accepted 2,060 and rejected 825 requests. DSS granted 1,301 final FCLs and 287 interim FCLs.[2] DSS discontinued 527 FCLs and terminated 1,155 FCLs.

- In FY14, DSS received 2,782 FCL sponsorship requests, of which DSS accepted 1,860 and rejected 922. DSS granted 1,137 final and 332 interim FCLs. DSS discontinued 535 FCLs and terminated 1,333 FCLs.

- In FY13, DSS approved final Top Secret FCLs within an average of 139 days of receiving the request, final Secret and Confidential FCLs in 148 days, and interim FCLs in an average of 91 days.

- In FY14, DSS approved final Top Secret FCLs within an average of 125 days, final Secret and Confidential FCLs in 137 days, and interim FCLs in an average of 93 days.

- NISP information assurance activities:

    - The DSS Office of Designated Approving Authority (ODAA) in the IO Directorate maintains over 10,555 active accredited system plans across the country at over 13,114 cleared contractor sites.

[1] An FCL sponsorship request involves the submission of a letter by a government contracting activity or a currently cleared contractor sponsoring an uncleared company. The letter must show justification that the company must need access to classified information in connection with a legitimate U.S. or foreign government requirement. The sponsorship request effectively begins the facility clearance process.

[2] The final FCL cannot be issued unless all key management personnel have received a favorable and final personnel security eligibility determination and the facility has met all other FCL requirements in accordance with the NISPOM. DSS may grant eligible contractors an interim FCL on a temporary basis pending completion of the final personnel security eligibility determinations for key management personnel.

- ODAA issued 2,202 interim approvals to operate (IATOs) from October 2013 through September 2014. It took an average of 21 days to process security plans from receipt to issuance of the IATO.

- ODAA issued 3,342 approvals to operate (ATOs) from October 2013 and September 2014. Of these, 44 percent (1,455) were processed "Straight to ATO."

- ATOs issued via the standard process took an average of 105 days to advance from IATO to ATO.

  - Systems processed Straight to ATO took an average of 25 days.

  - This process mitigates the risk assumed with systems operating on IATOs.

- NISP command cyber readiness inspection (CCRI) activities/metrics:

  - DSS oversees contractors' administration of 170 accredited cleared industry SIPRNet connections subject to CCRIs.

    - In FY14, DSS conducted 26 industry CCRIs.

    - DISA personnel led 24 and DSS personnel led 2 of these inspections.

  - DISA approved three DSS teams in FY14 to conduct CCRIs on behalf of U.S. Cyber Command. DSS has 18 ISSPs and 6 ISRs eligible to conduct CCRIs.

- An "acute/critical" security vulnerability is substantial and could result, or has resulted, in the loss or compromise of classified information. Of the security vulnerabilities found by DSS in cleared industry during FY14, 8 percent were acute/critical vulnerabilities, compared to 9 percent in FY13.

- The DSS CI Directorate continued to measure success in terms of the number of known/suspected collectors identified per CI resource. By the end of FY14, the CI Directorate identified 989 possible collectors for investigation or other action — a substantial increase over the 717 identified in FY13. This equates to 6.3 actions per CI resource. Based on these numbers, DSS estimates there are 1,400 known or suspected collectors exploiting their access and 11,000 vulnerabilities annually.

Topic II: A description of funds authorized, appropriated, or reprogrammed to carry out the requirements of this section, the budget execution of such funds, and the adequacy of budgets provided for performing such purpose.

The Department funded $101.189 million for FY13 requirements and $110.6 million for FY14 requirements to perform NISP oversight. The FY13 and FY14 budgets were adequate to perform mission requirements.

DSS Funding for Major Programs
Fiscal Years 2013 and 2014
(actuals in millions of dollars)

	FY13	**FY14**
NISP[3]	$101,189	$110,562
CI	$26,666	$24,073
PSI-I[4]	$222,000	$255,000
CDSE	$28,351	$26,648
TOTALS	$378,206	$421,051

Note: Section 347 of the John Warner National Defense Authorization Act for FY07 required the Secretary of Defense to include, in the budget justification documents submitted to Congress in support of the President's budget for the Department of Defense for each fiscal year, a report on the Department's future requirements with respect to Personnel Security Investigations for Industry (PSI-I) and with respect to the NISP activities of the Defense Security Service. This requirement was rescinded in Section 1062(d) of the FY12 NDAA. While the original reporting requirement was rescinded, the Department believes the following data concerning the PSI-I program funding may still be of interest to the Congress.

PSI-Is are centrally funded through the Defense-wide Operations and Maintenance Appropriation. The Department will continue to work closely with cleared industry to track any changes in projections and will continue highlighting the importance of responding to the DSS ongoing PSI-I Requirements Surveys.

The actual amount expended for PSI-I in FY13 was $222.0 million and in FY14 was $255.0 million. The Department budgeted $242.1 million for FY15 requirements and has

[3] NISP funding includes funding for both the IO and IP Directorates for the reporting period.

[4] PSI-I funding refers to direct reimbursable costs charged by the Office of Personnel Management to conduct personnel security investigations for persons working for contractors cleared under the NISP. DSS pays OPM for these expenses on behalf of the Department of Defense and 27 other Federal agencies that obtain NISP services from the Department.

requested $241,300 million in PSI-I funding for FY16. The Department will review PSI-I execution in FY15 and address FY17-20 PSI-I requirements during the FY17 budget cycle.

- FY17: $191,500 million
- FY18: $194,800 million
- FY19: $198,900 million
- FY20: $199,635 million

Topic III: Statistics on the number of contractors handling classified information of the Department of Defense, and the percentage of such contractors who are subject to foreign ownership, control or influence.

As of September 30, 2014:

- There are approximately 851,000 individuals in industry who hold clearance eligibility and 13,114 facilities cleared under the NISP.

- There are 701 cleared facilities with current FOCI mitigation instruments in place because DSS deemed the U.S. companies that maintain those facilities to be under FOCI.

- Based on the total cleared population, 5.3 percent of cleared facilities are cleared under the auspices of a FOCI mitigation agreement.

- There are 288 FOCI agreements in place.

- There are nine companies in various stages of the FOCI mitigation process without current agreements in place. The number of companies in process varies as new cases are opened and resolved.

- The average number of days to implement a FOCI mitigation plan is 93 days.

Topic IV: Statistics on the number of violations identified, enforcement actions taken, and the percentage of such violations occurring at facilities of contractors subject to foreign ownership, control, or influence.

Instances of noncompliance with NISPOM requirements (hereafter referred to as "vulnerabilities") found during assessments are categorized as either "acute/critical" or "non-acute/critical" vulnerabilities. Acute/critical vulnerabilities are substantial vulnerabilities that could result, or have resulted, in loss or compromise of classified information. Examples include process or system failures, such as processing classified information on a non-accredited information system, and transmitting classified information over unsecured lines.

Non-acute/critical vulnerabilities are those conditions that violate a NISPOM requirement but do not directly place classified information at risk of loss or compromise. Examples include incomplete visitor logs, lack of signatures on briefing statements, and the absence of initials on audit trail review checks. Available data on non-acute/critical vulnerabilities also includes those vulnerabilities corrected during a DSS assessment (i.e., corrected on the spot). All vulnerabilities noted by DSS during assessments are reflected in a written report that refers to the applicable NISPOM paragraph and include a corrective action required by DSS. The NISPOM provides detailed requirements for the contractors' industrial security programs, and is incorporated into those U.S. Government contracts that require the contractor to have access to classified information or technology during the performance of the contract.

Of the acute/critical vulnerabilities found during DSS assessments, the most commonly found during the reporting period were:

- Failure to provide security training to cleared employees commensurate with their involvement with classified information.

- Uncleared persons in key management positions (e.g., president/chief executive officer).

- Operating an information system processing classified information without proper approval.

- Failure to meet security audit requirements for information systems processing classified information.

- Classified information lost or compromised and not reported to DSS.

The chart below reflects data captured by DSS for the reporting period.

Summary of DSS Security Assessments of Cleared Facilities
October 1, 2012, to September 30, 2014

	All Cleared Facilities		**Facilities with FOCI Mitigation**	
Assessment Summary	**FY 13**	**FY14**	**FY 13**	**FY14**
Security assessments conducted at cleared facilities	**7,203**	**6,783**	**646**	**586**
Security assessments which identified vulnerabilities	**3,631**	**3,522**	**301**	**287**
Total security vulnerabilities identified during assessments*	**11,237**	**10,856**	**995**	**928**
Non-acute/critical vulnerabilities	**10,195**	**10,013**	**920**	**848**
Acute/critical vulnerabilities	**1,042**	**843**	**75**	**80**
Projected unidentified and unmitigated vulnerabilities	**9,797**	**10,737**	**269**	**384**
Non-acute/critical vulnerabilities	**8,887**	**9,903**	**250**	**351**
Acute/critical vulnerabilities	**910**	**834**	**19**	**33**
Total enforcement actions taken				
Marginal security ratings	**10**	**22**	**1**	**3**
Unsatisfactory security ratings	**31**	**35**	**4**	**5**
Facility clearance invalidations	**57**	**58**	**3**	**15**

*****_Since March 2012, DSS has performed follow-up contact regarding all identified vulnerabilities to ensure the contractor facility has applied appropriate mitigation action, and has tracked facilities' completion of those mitigations in a DSS internal database. The goal for completing mitigation actions is 15 days for acute/critical vulnerabilities and 30 days for non-acute/non-critical vulnerabilities. In FY13 and FY14, approximately 9 percent of the total assessments DSS conducted were done at facilities with FOCI mitigation agreements in place. During FY13, vulnerabilities found at FOCI facilities accounted for 9 percent of the total; however, in FY14 this percentage dropped to 8 percent, showing a slight reduction in the number of vulnerabilities at FOCI facilities._

Background

Once a facility is cleared under the NISP, DSS evaluates the NISP security operations of the organization. At the completion of every security assessment, DSS assigns a security rating. The security ratings are defined as follows:

- The "Superior" security rating is reserved for cleared facilities that have consistently and fully implemented the requirements of the NISPOM in an effective fashion, resulting in a security posture of the highest caliber compared with other cleared facilities of similar size and complexity. A cleared facility assigned a rating of “Superior” must have documented and implemented procedures that heighten the security awareness of company employees and must foster a spirit of cooperation within the security community. This rating also requires that a sustained high level of management support must be present for the security program.

- The “Commendable” security rating is assigned to cleared facilities that have fully implemented the requirements of the NISPOM in an effective fashion, resulting in an exemplary security posture compared with other cleared facilities of similar size and complexity. This rating denotes a security program with strong management support, the absence of any acute/critical security issues, and only minor non-acute/critical vulnerabilities.

- The “Satisfactory” security rating is the most common and denotes that a cleared facility’s security program is in general conformity with the basic requirements of the NISPOM. This rating can be assigned even if there were vulnerabilities requiring corrective action in one or more of the security program elements within the cleared facility’s overall security program. Depending on the circumstances, a satisfactory rating can be assigned even if there were isolated acute/critical vulnerabilities during the security review.

- The “Marginal” security rating is assigned when a cleared facility’s security program is not in general conformity with the basic requirements of the NISPOM. This rating signifies an acute/critical vulnerability in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected.

- The “Unsatisfactory” security rating is assigned when circumstances and conditions indicate that the cleared facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating is appropriate when the security assessment results indicate the cleared facility can no longer credibly demonstrate that it can reliably preclude the disclosure of classified information to unauthorized persons.

For facilities that receive a marginal or unsatisfactory security rating, DSS conducts compliance reassessments to identify and review corrective actions. DSS views compliance reassessments as an enforcement action and completes them within 120 days after a facility receives a marginal rating and within 60 days after a facility receives an unsatisfactory rating.

DSS also has the authority to take the additional enforcement actions of invalidating or revoking a facility clearance. These actions may be taken as a result of a security assessment or compliance assessment, or if DSS becomes aware of information about or actions by the cleared company which adversely affect its ability to protect classified information or its eligibility for a facility clearance. Invalidation of a facility clearance is an interim measure taken by DSS to allow the cleared company to correct the circumstances that negate the integrity of the cleared company’s security program. Invalidation allows the facility to continue to perform on existing classified work with the concurrence of their government contracting activities, but prohibits the facility from bidding on or accepting new work. When invalidating a facility clearance, DSS sets a specific deadline for corrective actions to be taken and follows up to determine whether revalidation or revocation of the facility clearance is necessary.

Revocation of a facility clearance is the most severe enforcement action DSS can take against a facility. Revocation of a facility clearance terminates a cleared company's facility security clearance, rendering it ineligible to perform on classified contracts or access classified information. DSS coordinates revocation decisions with the affected government contracting activities.

Topic V: An assessment of whether major contractors implementing the program have adequate enforcement programs and have trained their employees adequately in the requirements of the program.

The Department does not have a definition as to what constitutes a "major" contractor. Therefore, the data in this report is consolidated for all facilities cleared under the NISP.

Of the facilities assessed by DSS during the reporting period, DSS rated 99 percent "Satisfactory or better," indicating that they are effectively protecting classified information. To achieve a "Satisfactory" security assessment rating, contractors must have security enforcement and training programs that conform to NISPOM requirements.

A good relationship between DSS and industry depends upon productively balancing cooperation and partnership with strong enforcement and oversight. The DSS workforce is expected to be professional in all dealings with companies, and DSS wants cleared companies to be successful in their security programs.

A company's commitment to implementing the NISP effectively is demonstrated in the establishment and operation of a security program which consistently and fully implements NISPOM requirements effectively. Achieving a "Satisfactory" or higher rating requires a sustained high level of management support for the security program. For instance, the following are examples of facility behavior DSS considers in making its determinations about the effectiveness of a company's security program:

- Demonstrated management support and cooperation with the facility security officer (FSO).

- Personal involvement of management in facility security education and awareness programs.

- Absence of any acute/critical vulnerabilities that impact integrity of security systems in place.

- Effective security staff who conduct thorough non-acute/critical inquiries with prompt reporting, quality investigations, and implementation of appropriate corrective actions when violations are discovered.

- Information systems security personnel appropriately trained in the technologies of the systems under their responsibilities.

To better direct its resources, DSS continues to refine its threat mitigation strategy and methodology to prioritize assessments to better incorporate assessments of counterintelligence threats to cleared U.S. companies. The goal is a coordinated, integrated visit from DSS to the right facility at the right time, with appropriate resources, resulting in a more effective and meaningful assessment.

DSS has established an assessment methodology that applies an evolutionary threat mitigation strategy and methodology to prioritize assessments. This prioritization is based on quantitative risk management factors and serves as the agency's primary assessment of risk as it relates to the overall foreign threat to key technologies within cleared companies. This ensures that the most important or highest risk facilities receive the greatest scrutiny and are expected to have the most stringent security programs.

Topic VI: Trend data on attempts to compromise classified information disclosed to contractors of the Department of Defense to the extent that such data are available.

The CI Directorate annually produces classified and unclassified reports detailing foreign attempts to illicitly acquire information or technology in cleared industry, entitled "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry." These reports are based on analysis of suspicious contact reports received from cleared companies and identify the most frequently targeted U.S. technologies, reflect the most common collection methods utilized, identify entities attempting the collection, and identify the countries/regions where these collection efforts originate.

Other analytical products include company and program-based assessments, threat advisories and training and educational materials. The company assessments provide a specific cleared company with current information about the threat posed to information and technology resident at its facilities. The program assessments identify the foreign collection threat to a specific defense program.

The most recent unclassified version of the annual Trends report is attached. The classified versions of this report and the quarterly assessments are available upon request.

The unclassified version of the Trends report is also available on the DSS website at: http://www.dss.mil/documents/ci/2014UnclassTrends.PDF

APPENDIX A – TRAINING, EDUCATION, AND CERTIFICATION

DSS offers 53 instructor-led and eLearning courses related to industrial security, cybersecurity, and CI awareness. During the reporting period, DSS personnel with Industrial Security Program oversight responsibilities participated in and completed 9,077 training courses and 93 achieved the Industrial Security Oversight Certification. Also, industry personnel participated in and completed 75,189 training courses and 5 achieved the Industrial Security Oversight Certification. The table below provides detailed course and completion information for the reporting period.

Industrial Security Course Completions
October 1, 2012, to September 30, 2014

Course	Description	DSS Attendees	Industry Attendees
AA&E Facility Physical Security Inspection Exercise	Provides an opportunity to apply knowledge of regulatory requirements for physical security measures and facility standard practices procedures in a realistic, three-dimensional environment.	2	9
Business Structures in the NISP	Covers the most common business structures ISRs encounter when processing a company for a facility clearance	101	484
CI Awareness and Reporting for DoD	DoDD5240.06 Counterintelligence Awareness and Reporting	133	1871
CI Awareness and Reporting for DSS	DoDD5240.06 Counterintelligence Awareness and Reporting (required annual training)	1600	0
Cybersecurity Awareness	Introduces the automated information systems environment and the threats and vulnerabilities faced when working within the government or defense industrial systems.	162	6853
Derivative Classification	Explains how to derivatively classify national security information from a classification management perspective	190	9453

Course	Description	DSS Attendees	Industry Attendees
Developing a Security Education Program	Provides a thorough overview of the DoD and NISP policy requirements, best practices, and instructional methods for developing and implementing a security education program	167	2746
DSS Security Rating Process Course	Provides the student with an overview of the standardized DSS process for assigning a security rating using the DSS Security Rating Matrix.	103	359
eFCL for DSS users	This was developed to assist persons who use the eFCL Submission Site. Companies are required to use eFCL to submit facility clearance applications and changed conditions to DSS in electronic format	85	71
Essentials of Industrial Security Management	Covers basic NISP requirements with emphasis on cleared contractor responsibilities	4	133
Establishing an Insider Threat Program for Your Organization	Guide for new Insider Threat Program Managers	33	362
Facility Clearances in the NISP	The Facility Clearances in the NISP course introduces the student to the purpose and the eligibility requirements of an FCL. The course covers the FCL request process as well as the impact the various business structures and the impact that certain changed conditions and personnel actions may have on an FCL	182	3033
FSO Role in the NISP	Describes the role of the FSO in the NISP	178	2580
Fundamentals of Industrial Security	The course provides new ISRs with a baseline understanding of the requirements and core responsibilities of the DSS industrial security mission.	39	0
Getting Started Seminar for New FSOs	Provides new FSOs with an opportunity to apply fundamental NISP requirements	10	245

Course	Description	DSS Attendees	Industry Attendees
Industrial Security Facilities Database (ISFD) Facility Clearance Verification and Notifications for Industry v3	Provides step-by-step instructions on the use of the ISFD's Facility Verification Request application feature to verify the status of an FCL	225	3424
Information System Security in the NISP	This course covers the DSS/ODAA Certification and Accreditation (C&A) Process, including the configuration of computers based on the security standards in Chapter 8 of the NISPOM and the Standardization of Baseline Technical Security Configurations (published by DSS).	6	119
Insider Threat Awareness	National Insider Threat Policy Minimum Standards/DoD Directive 5205.16 (required initial and annual training)	969	1528
Integrating CI and Threat Awareness	Provides thorough overview of CI and threat awareness, essential components of a comprehensive security program	203	2679
Intelligence Oversight	DoDD 5240.1-R Annual Intelligence Oversight training for DSS personnel. One track for CI and second track for non-CI personnel.	1723	96
Introduction to Industrial Security	Provides an introduction to the DoD Industrial Security Program	193	1157
Introduction to the NISP Certification and Accreditation Process	This course introduces the NISP Certification and Accreditation process. The course provides training on the policies and standards used to protection information within computer systems in support of the DSS mission	181	1235
Introduction to the Risk Management Framework	Introduces the Risk Management Framework and Cybersecurity policies for the Department of Defense.	12	45

Course	Description	DSS Attendees	Industry Attendees
ISFD for DSS Users v3	Provides step-by-step instructions on the use of the ISFD. Students practice populating and manipulating the ISFD in a virtual classroom environment that simulates the functionality of the real-time database	88	6
JPAS/JCAVS Training for Security Professionals	Provides an overview of the Joint Personnel Adjudication System (JPAS) and a detailed explanation of its subsystem, the Joint Clearance and Access Verification System (JCAVS) used by DoD personnel security managers and FSOs for eligibility and investigation verification	328	6048
JPAS/JCAVS Virtual Training online course	Provides an overview of JPAS and a detailed explanation of its subsystem, JCAVS, which are used extensively by DoD personnel security managers and FSOs for eligibility and investigation verification	365	6562
Marking Classified Information	Examines the requirements and methods for marking classified documents and other classified material	186	2298
Mission Assurance for Senior Leaders	Improve senior leaders' awareness about the seriousness of cybersecurity as it relates to their actions, as well as the implications of those actions on national security, DoD information, the organization's mission, and the senior leader's various social networks.	0	4
NISP Certification and Accreditation C&A Process: A Walk-Through Course	This course is a continuation of the Introduction to the NISP C&A Process Course (IS100.16). This course identifies in depth the individual phases of DSS C&A process	92	761
NISP Information Assurance Fundamentals	The course provides ISSPs with a baseline understanding of the requirements and core responsibilities of the DSS industrial security mission.	11	
NISP Reporting Requirements	This course introduces the reporting requirements as outlined in NISPOM 1-300	173	2964

Course	Description	DSS Attendees	Industry Attendees
NISP Self Inspection	Focuses on how to conduct a self-inspection	153	2706
OBMS – Contractor Submitter	Provides training on the functionality for the Contractor Submitter role within the ODAA Business Management System (OBMS).	15	126
OBMS – Government Submitter	Provides training on the functionality for the Government Submitter role within OBMS.	10	3
OBMS – Internal Non-ODAA	Provides training on the functionality for internal DSS Non-ODAA personnel within OBMS.	18	0
OBMS – Internal ODAA	Provides training on the functionality for internal DSS ODAA personnel within OBMS.	37	0
Personnel Clearances in the NISP	This course includes instruction on the personnel security requirements for contractors participating in the NISP and how those requirements are implemented by DoD	198	2922
Phishing Awareness	Provides an explanation of what phishing is, as well as examples of the different types of phishing.	119	247
Portable Electronic Devices / Removable Storage Media	Information systems users will learn about significant security risks associated with portable electronic devices and removable storage media.	6	75
Privileged User IA Responsibilities	Presents the additional IA responsibilities for information system users with access privileges elevated above those of an authorized user.	3	71

Course	Description	DSS Attendees	Industry Attendees
Protecting Your Facility's Technology	Understanding technology being protected within facility.	3	8
Relationship Between CI and Security	Counterintelligence fundamentals for FSOs	22	99
Safeguarding Classified Information in the NISP	Covers the rules and procedures for protecting classified information and material in the NISP	111	1546
Sensitizing Your Employees to CI Concerns	CI fundamentals for cleared contractors	17	106
Smartphones and Tablets	The "Awareness" course provides students with information about the security risks and vulnerabilities associated with using smartphones and tablet devices.	8	175
Suspicious Emails	Recognizing and reporting suspected unsolicited collection attempts via emails	3	8
The Technical Implementation of C&A – Configuration to DSS Standards Course	This course focuses on the more technical aspects of the C&A process and guides students on navigating through the system using the Baseline Technical Security Configuration Guide	83	611
The Technical Implementation of C&A – Configuration to DSS Standards Virtual Environment	The Virtual Environment provides the opportunity for students participating in the Technical Implementation of C&A: Configuration to DSS Standards course to practice what they have learned in a Non-Production/Test environment	57	466

Course	Description	DSS Attendees	Industry Attendees
Thwarting the Enemy	Understanding NISPOM 1-300, which requires cleared companies to report suspicious activities		2023
Transmission and Transportation for Industry	Examines the requirements and methods for transmitting or transporting classified information and other classified material in accordance with NISP	106	1426
Understanding Foreign Ownership, Control or Influence (FOCI)	This course introduces important FOCI terms and processes as they relate to the Industrial Security Program and describes the foundational four major components of the FOCI process: identification, adjudication, mitigation and inspection	166	2697
Visits and Meetings in the NISP	Covers the rules and procedures for classified visits and meetings for cleared companies participating in the NISP	134	2633

Note: While not included in the above chart, in FY13, there were 162,019 course completions for DoD civilian employees and 115,062 course completions for military personnel, for a total of 277,081 course completions. In FY14, there were 171,198 course completions for DoD civilian employees and 117,970 course completions for military personnel, for a total of 289,168 course completions.

APPENDIX B – REPORT LANGUAGE

PL 110-417 BIENNIAL REPORT ON IMPROVING INDUSTRIAL SECURITY

‘‘(f) BIENNIAL REPORT.—The Secretary shall report biennially to the congressional defense committees on expenditures and activities of the Department of Defense in carrying out the requirements of this section. The Secretary shall submit the report at or about the same time that the President’s budget is submitted pursuant to section 1105(a) of title 31, United States Code, in odd numbered years. The report shall be in an unclassified form (with a classified annex if necessary) and shall cover the activities of the Department of Defense in the preceding two fiscal years, including the following:

‘‘(1) The workforce responsible for carrying out the requirements of this section, including the number and experience of such workforce; training in the performance of industrial security functions; performance metrics; and resulting assessment of overall quality.

‘‘(2) A description of funds authorized, appropriated, or reprogrammed to carry out the requirements of this section, the budget execution of such funds, and the adequacy of budgets provided for performing such purpose.

‘‘(3) Statistics on the number of contractors handling classified information of the Department of Defense, and the percentage of such contractors who are subject to foreign ownership, control, or influence.

‘‘(4) Statistics on the number of violations identified, enforcement actions taken, and the percentage of such violations occurring at facilities of contractors subject to foreign ownership, control, or influence.

‘‘(5) An assessment of whether major contractors implementing the program have adequate enforcement programs and have trained their employees adequately in the requirements of the program.

‘‘(6) Trend data on attempts to compromise classified information disclosed to contractors of the Department of Defense to the extent that such data are available.’’