Biennial Report to Congress on Improving Industrial Security

U.S. Department of Defense

February 2013

The estimated cost of report or study for the Department of Defense is approximately $21,000 for the 2013 Fiscal Year. This includes $3,410 in expenses and $17,000 in DoD labor.
Generated on 2013Mar19 RefID: 3-5763ECF

Biennial Report to Congress on
Improving Industrial Security

This report complies with section 428 of title 10, U.S.C., 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 years 2011 and 2012.

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 DSS planned workforce for fiscal years 2011 and 2012 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	**FY 2011 - AUTH**	**FY 2011 - ACTUAL**	**FY 2012 - AUTH**	**FY 2012 - ACTUAL**
Industrial Security Field Operations (IO)	388	383	401	372
Industrial Security Policy and Programs (IP)	61	57	61	56
Defense Industrial Security Clearance Office (DISCO)	125	98	118	110
DSS Counterintelligence Office (CI)	96	136	86	127
Center for Development of Security Excellence (CDSE)[1]	61	73	74	65
TOTALS	731	747	740	730

IO is an organizational element of DSS that works with cleared companies across the United States to ensure the protection of classified information. IO is comprised of industrial security representatives (ISRs), who are general security specialists, as well as

[1] Previous reports to Congress did not include manpower figures for CDSE. However, given the role the CDSE plays in delivering training and education to the industrial security community, including cleared contractors under the National Industrial Security Program, DoD considers these figures to be of interest and relevant to this report.

information systems security professionals (ISSPs), who are technical experts who accredit industry information systems in cleared industry to process classified information. IO also includes a headquarters element that oversees field personnel, processes and grants requests for facility clearances (FCLs) and monitors conditions affecting FCLs.

DISCO makes determinations regarding the eligibility of contractors and contractor personnel for access to classified information, and processes industrial clearance and personnel security investigative actions. These actions include adjudicating personnel security investigations (PSIs) for contractor personnel under the NISP; processing international clearances, overseas assignments, international visit requests, and international transactions relating to personnel and facility clearance verifications; issuing NATO Facility and Personnel Certificates; and overseeing contractor employees' continued eligibility for access to classified information.

On May 3, 2012, the Deputy Secretary of Defense directed a complete consolidation of the functions, resources, and assets of the Army Central Clearance Facility, Department of the Navy Central Adjudication Facility (CAF), Air Force CAF, Joint Staff CAF, Washington Headquarters Services CAF, Defense Industrial Security Clearance Office, and the Defense Office of Hearings and Appeals into a single organization under the authority, direction and control of the Director of Administration and Management. As of October 22, 2012, DoD realigned DISCO under the DoD consolidated CAF and DSS no longer adjudicates personnel security clearance eligibility for industry personnel under the NISP. DSS will retain all other functions associated with personnel security management for industry to include review and submission of the Electronic Questionnaires or Investigations Processing (e-QIP), personnel security management and oversight for industry, international visit requests and security assurances, as well as statistical analysis and funding of the PSI program for industry.

IP is an organizational element of DSS that adjudicates Foreign Ownership, Control or Influence (FOCI) issues, administers international programs, and provides industrial and personnel security policy guidance to industry. As part of IP's FOCI mission, DSS provides input to the DoD lead for the Committee on Foreign Investment in the United States (CFIUS) on all covered CFIUS transactions to determine if the transactions involve FOCI jurisdiction under the National Industrial Security Program Operating Manual (NISPOM).

The DSS CI Directorate identifies known or suspected collectors involved in illicit attempts to obtain classified U.S. government information resident in the defense industrial base (DIB) and articulates the CI threat to industry. The DSS CI Directorate refers incidents indicating possible attempts to steal sensitive technology to national counterintelligence and law enforcement (LE) agencies for investigative follow-up or operational exploitation.

DSS CI specialists work in partnership with industry, other DSS stakeholders, and the LE and intelligence communities (IC) to: determine hostile involvement, refer CI-relevant information reported by cleared industry to the IC and LE, identify and educate cleared industry on intelligence collection trends and threats, and provide a baseline for effective countermeasures to protect U.S. classified information and technologies and programs at risk to foreign or hostile targeting. DSS CI also leverages national CI and Federal LE resources to effectively deter, investigate, neutralize, or exploit penetration attempts strengthening cleared industry as the ‘first line of defense’ against a pervasive and growing threat. DSS is working closely with cleared industry to ‘take back the initiative’ and prevent the loss of critical program information.

The Center for Development of Security Excellence (CDSE) provides the Department of Defense with a security center of excellence for the professionalization of the security community and is the premier provider of security education and training for the Department of Defense and industry.

The Education Division of CDSE develops college-level and graduate courses and workshops for DoD security professionals who are advancing their professional growth. This division is responsible for the development of courses for advanced security studies in support of the Security Professional Education Development Certification Program. The Education Division is also responsible for facilitating the evaluation of CDSE courses for college credit equivalencies.

The Training Division of CDSE provides security training to DoD and other U.S. Government personnel, employees of U.S. Government contractors, and when sponsored by authorized DoD Components, employees of foreign governments. The Training Division creates, collaborates and facilitates delivery of quality training across the Industrial, Information, Personnel, and Physical security disciplines, as well as other security-related areas such as Special Access Programs. Training is delivered through a variety of formats to include resident courses, mobile courses delivered at activities located within or outside the United States, eLearning courses, audio podcasts, webinars, virtual simulations, and performance support tools accessed online via the CDSE website and its Learning Management System. The training division also operates the Defense Security Service Academy (DSSA) which provides security training for industrial security professionals within the Defense Security Service.

DSS is constantly evaluating its training and assessing the quality of its workforce and is confident it has a high quality, high performing workforce. All new ISRs and ISSPs assigned to DSS participate in a formal mentoring program with more experienced personnel. They participate in a formal training program divided into two parts. The Fundamentals of Industrial Security Level 1(FISL 1) is an interactive, blended learning format course consisting of web-based training, mentoring, structured field activities, some of which are evaluated by instructors, on-the-job training, and formal assessments. The course provides new ISRs and ISSPs with a baseline understanding of the requirements and core responsibilities of the DSS industrial security mission. It focuses on the teaching of industrial security requirements and internal DSS processes and procedures to prepare the ISR and ISSP to perform independently in the field.

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

Field counterintelligence specialists (FCISs) are typically hired into DSS with extensive backgrounds in CI and LE, and have typically served in credentialed CI or federal LE positions within the military services or other U.S. government agencies. Additional training is provided to FCISs and headquarters intelligence analysts via the Joint Counterintelligence Training Academy, or through other IC training sources.

During the reporting period, DSS personnel with Industrial Security Program oversight responsibilities participated in and completed 2,930 industrial security training courses. In addition, industry personnel participated in and completed 30,200 industrial security training courses. Detailed information describing these training courses is contained in Appendix A.

DSS undertook a number of initiatives during the reporting period to improve its oversight of the NISP. These initiatives are outlined in Appendix B.

DSS established metrics to measure its performance in the oversight and administration of the NISP. The metrics are designed to let DSS know how it is using its resources and to troubleshoot problem areas. To gather this information, DSS has developed a method of data calls across the agency to collect and compile the information. The following are examples of the metrics DSS gathers to monitor its performance. All information is current as of September 30, 2012. (NOTE: “days” refers to calendar days.)

- In FY11, DSS received 2,800 facility clearance (FCL) sponsorship requests[2], accepted 2,100 FCL sponsorship requests and rejected 729 FCL sponsorship

[2] 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

requests. DSS granted 1,271 final FCLs and 293 interim FCLs[3]. DSS discontinued 546 FCLs and terminated 1,456 FCLs.

- In FY12, DSS received 3,169 FCL sponsorship requests, accepted 2,092 FCL sponsorship requests and rejected 1,077 FCL sponsorship requests. DSS granted 1,558 final facility clearances (FCLs) and 410 interim FCLs. DSS discontinued 613 FCLs and terminated 1,352 FCLs.

- In FY11, DSS approved final top secret FCLs within an average of 156 days, approved final secret and confidential FCLs within an average of 131 days and approved interim clearances within an average of 64 days.

- In FY12, DSS approved final top secret FCLs within an average of 158 days, approved final secret and confidential FCLs within an average of 178 days and approved interim clearances within an average of 108 days.

- NISP Certification and Accreditation (C&A) activities/metrics
  - DSS Office of Designated Approving Authority (ODAA) maintains an inventory of over 12,000 active accredited system plans located across the country at over 2,000 cleared contractor sites.
  - DSS ISSPs also provide oversight of 800 unclassified system Electronic Control Plans (ECPs) at FOCI company sites.
  - ODAA issued 2,479 interim approvals to operate (IATOs[4]) between October 2011 and September 2012.
    - It took an average of 15 days to process security plans from receipt to IATO.
  - ODAA issued 4,095 approvals to operate (ATOs[5]) between October 2011 and September 2012.
    - 41% of these ATOs were processed “Straight to ATO.”
    - ATOs issued via the standard process took an average of 83 days to go from IATO to ATO
    - The 41% (1698) systems processed Straight to ATO took an average of 14 days

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.

[3] The final FCL shall not be issued unless all KMP have received a favorable and final eligibility determination and the facility has met all other FCL requirements in accordance with the National Industrial Security Operating Manual (NISPOM). An interim FCL may be granted by DSS to eligible contractors on a temporary basis pending completion of the final personnel security eligibility determinations for the key management personnel.

[4] An interim approval to operate (IATO) allows the cleared contractor to begin processing classified materials on their information systems until a final authority to operate is issued.

[5] After an assessment of the contractor’s protective security measures, DSS will issue an approval to operate (ATO) or a final accreditation to process or continue processing classified materials on their information systems.

  - This process mitigates the risk assumed with systems operating on IATO

- An “acute/critical” security vulnerability (termed as a “serious deficiency” in the 2011 report) is substantive in nature and could result in the loss or compromise of classified information. Of the security vulnerabilities found in FY12, 8.7 percent were acute/critical findings, compared to FY11, with 7 percent.

- DSS CI continued to measure success in terms of the number of known/suspected collectors identified per CI resource. By the end of FY12, DSS CI identified 657 possible collectors for investigation or other action—a substantial increase over the 201 identified in FY10. For FY12, DSS CI set a goal to identify 3.0 collectors for every CI full-time employee (FTE), an increase from the goal of identifying 1.5 collectors in FY10. In August 2012, the rate of identification was as high as 5.0 per FTE, up from 1.99 in FY10.

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.

DoD funded $88.7 million for FY11 requirements and $110.2 million for fiscal year 2012 requirements to perform NISP oversight. The FY11 and FY12 budgets were adequate to perform mission requirements.

DSS Funding for Major Programs
Fiscal Years 2011 and 2012
(actuals in millions of dollars)

	FY11	FY12
NISP[6]	88.7	110.2
CI	24.9	23.9
PSI-I[7]	240.5	252.2
CDSE	22.4	25.3
TOTALS	376.5	411.6

Note: Section 347 of the John Warner National Defense Authorization Act for Fiscal Year (FY) 2007, 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 (DoD) for each fiscal year, a report on the future requirements of DoD with respect to Personnel Security Investigations for Industry (PSI-I) and with respect to the National Industrial Security Program (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.

[6] NISP funding includes funding for both the Industrial Security Field Operations (to include DISCO) and Industrial Security Policy and Programs Offices for the reporting period.

[7] PSI-I funding refers to direct reimbursable expenditures to the Office of Personnel Management to conduct investigations for individuals cleared under the National Industrial Security Program. DSS reimburses OPM for these expenses on behalf of the Department of Defense and 24 other Federal Agencies.

The actual amount expended for PSI-I in FY11 was $240.5 million. The actual amount expended for PSI-Is in FY12 was $252.2 million. DoD budgeted $241.0 million for FY13 requirements. In addition, DoD has approved $278 million PSI-I funding for FY14. The Department will review PSI-I execution in FY13 and address FY15-FY18 PSI-I requirements during the FY15 budget cycle.

- FY15: $218.5 million
- FY16: $213.1 million
- FY17: $215.8 million
- FY18: $219.6 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.

All information is current as of September 30, 2012.

- There are approximately 940,000 active, cleared employees within the NISP.
- There are approximately 13,253 facilities cleared under the NISP.
- There are 747 cleared facilities with a current FOCI mitigation instrument in place. Based on the total cleared population, 5.6 percent of cleared facilities are cleared under the auspices of a FOCI mitigation agreement.
- At the end of FY12, there were 340 FOCI agreements in place. FY12 has 16% more agreements in place than in FY10.
- There are 72 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 render a decision on the appropriate method of FOCI mitigation is 149 days. This processing time has improved by 38 percent from 239 days in January 2009.
- During the reporting period, cases open for over 120 days decreased five percent from 23 cases to 22 cases. These 22 cases are included in the 72 total cases listed above which have not yet been mitigated.
- Internally, DSS allocated additional resources to increase the agency's capability for reviewing ownership structures and corporate relationships of companies entering the NISP in order to detect undisclosed elements of FOCI. In FY11, DSS conducted over 1,500 reviews, yielding nine percent with undisclosed elements of FOCI and five percent with counterintelligence concerns.

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 the National Industrial Security Operating Manual (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 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 (referred to as “administrative deficiencies” in 2011 report) are those conditions that violate a NISPOM requirement but do not directly place classified information at risk of loss or compromise. Some 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 the conduct of the inspection (i.e., corrected on the spot). All vulnerabilities noted by DSS during assessments are reflected in a written report that refers to the applicable paragraph in the NISPOM and include a recommended corrective action. These issuances state detailed requirements for the contractors’ industrial security programs and are incorporated by reference into the contracts issued to the cleared companies by U.S. Government agencies.

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

- Uncleared persons in key management positions
- 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 not reported to DSS

The chart below reflects data captured by DSS from October 1, 2010, through September 29, 2012.

Summary of DSS Security Assessments (referred to as "Security Inspections" in 2011 report) of Cleared Facilities
October 1, 2010, to September 29, 2012

	All Cleared Facilities		**Facilities with FOCI Mitigation**	
Assessment Summary	**FY 11**	**FY12**	**FY 11**	**FY12**
Security assessments conducted at cleared facilities	**9,222**	**8,043**	**723**	**701**
Security assessments which identified vulnerabilities	**4,790 (52%)**	**4,004 (50%)**	**381 (53%)**	**364 (52%)**
Total security vulnerabilities identified during assessments*	**16,322**	**11,785**	**1,159**	**1,146**
Count of non-acute/critical vulnerabilities	**15,031**	**11,785**	**1,159**	**1,146**
Count of acute/critical vulnerabilities	**1,291**	**1,057**	**111**	**102**
Total enforcement actions taken	**82**	**71**	**13**	**10**
Marginal security ratings	**19**	**19**	**2**	**4**
Unsatisfactory security ratings	**25**	**21**	**5**	**3**
Facility invalidations	**38**	**31**	**6**	**3**

Note: Since March, 2012, DSS has performed follow-up with all identified vulnerabilities to make sure they are mitigated by the contractor facility, and tracked their completions in its internal database. The goal for completion of mitigation of vulnerabilities is 15 days for Acute and Critical Vulnerabilities and 30 days for Non-Acute/Non-Critical Vulnerabilities. As a result of this new "find and fix" approach to assessments, DSS was not able to complete as many assessments in FY12 as it has in previous years. While DSS is unable to visit as many facilities, it is ensuring that the facilities it does visit are fully compliant with the NISP thereby mitigating the risk of vulnerabilities at these locations.

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 rating 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 the most acute/critical negative security rating. An unsatisfactory 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 review results indicate that the cleared facility can no longer credibly demonstrate that it can be depended upon to preclude the disclosure of classified information to unauthorized persons.

DSS conducts a compliance assessment to identify and assess the corrective actions taken by the cleared company at facilities that receive a Marginal or Unsatisfactory security rating. A compliance assessment is viewed by DSS as an enforcement action. The compliance assessment is completed within 120 days after the completion of the security assessment that led to the rating of “Marginal” and 60 calendar days after the completion of the security assessment that led to a rating of "Unsatisfactory."

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 appropriate 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.

Of the facilities assessed by DSS during the reporting period (October 1, 2010, through September 30, 2012), DSS rated 99.5 % “Satisfactory or better,” indicating that they are effectively protecting classified information. In order to achieve a “Satisfactory” security inspection rating, contractors must have security enforcement and training programs that conform to NISPOM requirements.

DoD 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.

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 the requirements of the NISP in an effective fashion. Achieving a “Satisfactory” rating or higher 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 security violations 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.

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 DSS CI Directorate produces a family of reports under the “Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry” titles. These DSS 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.

The Trends family of products includes a classified and unclassified version of the annual Trends product as well as a classified quarterly Trends product that focuses on a special topic area and relates the threat posed by a specific collection method of operation or the threat posed to a technology sector. Other new product lines are company- and program-based assessments. The company assessments provide a specific cleared company with 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 can also be found on the DSS website at: http://www.dss.mil/documents/ci/2012-unclass-trends.pdf

10 U.S.C. 428 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.’’

APPENDIX A - TRAINING

The following information is provided regarding the quality of training DSS offers.

During FY12, the DSS Center for Development of Security Excellence (CDSE) received college equivalency recommendation for four courses from the American Council on Education's Credit Recommendation Service (ACE CREDIT).

- Introduction to Special Access Programs – Two semester hours, lower division baccalaureate/associate degree category
- Special Access Programs Mid-Level Security Management – Three semester hours, upper division baccalaureate degree category
- Facility Security Officer Orientation for Non-Possessing Facilities Curriculum – Two semester hours, lower-division baccalaureate/associate degree category
- Facility Security Officer Program Management for Possessing Facilities - Two semester hours, lower division baccalaureate/associate degree category

In addition to course evaluation, ACE provides an office transcript to participants who successfully complete a course, examination or certification that has an ACE credit recommendation. This is an additional benefit to students, particularly those who may be considered for transfer by that institution.

DSS offers 31 online and instructor-led courses related to industrial security functions. During the reporting period, DSS personnel with Industrial Security Program oversight responsibilities participated in and completed 2,930 training courses, and industry personnel participated in and completed 30,200 training courses. The table below provides detailed course and attendance information for the reporting period.

Industrial Security Course Completions
October 1, 2010, to September 30, 2012

Course	Description	DSS Attendees	Industry Attendees
FSO Role in the NISP	Describes the role of the FSO in the NISP	278	4110
Getting Started Seminar for New FSOs	Provides new FSOs with an opportunity to apply fundamental NISP requirements	25	459

Essentials of Industrial Security Management	Covers basic NISP requirements with emphasis on cleared contractor responsibilities	136	1434
Introduction to Industrial Security	Provides an introduction to the DoD Industrial Security Program	188	949
Visits and Meetings in the NISP	Covers the rules and procedures for classified visits and meetings for cleared companies participating in the NISP	138	1302
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	14	104
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	125	1552
Safeguarding Classified Information in the NISP	Covers the rules and procedures for protecting classified information and material in the NISP	184	2010
Derivative Classification	Explains how to derivatively classify national security information from a classification management perspective	188	2238
Transmission and Transportation for Industry	Examines the requirements and methods for transmitting or transporting classified information and other classified material in accordance with NISP	127	1363
Marking Classified Information	Examines the requirements and methods for marking classified documents and other classified material	130	1228
Security Awareness For Educators (SAFE)	Addresses how to create an effective security awareness and education program and identifies solutions for overcoming the various challenges surrounding this responsibility	4	42

SAP Orientation	Introduces students to DoD Special Access Programs (SAPs)	33	149
NISPOM Chapter 8 Security Requirements	Introduces the security requirements for safeguarding classified information processed and stored in information systems at cleared company facilities	134	1124
NISPOM Chapter 8 Security Implementation	Teaches the basics of security for Local Area Networks and practices implementation of the security requirements described in Chapter 8 of the NISPOM	10	105
Business Structures in the NISP	Covers the most common business structures ISRs encounter when processing a company for a facility clearance	119	233
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	164	1700
Integrating CI and Threat Awareness	Provides thorough overview of CI and threat awareness, essential components of a comprehensive security program	143	1498
NISP Self Inspection	Focuses on how to conduct a self-inspection	115	1830
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 the DoD	87	1674
NISP Reporting Requirements	This course introduces the reporting requirements as outlined in NISPOM 1-300	77	1228
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	92	299

Facility Clearances in the NISP	The Facility Clearances in the NISP (FCL) 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	94	1373
eFCL for DSS users	This was developed to assist you when using the eFCL Submission Site. You will be required to use eFCL to submit facility clearance applications and changed conditions to DSS in electronic format	39	84
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	49	69
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	45	35
The Technical Implementation of C&A – Configuration to DSS Standards Virtual Environment	The Virtual Environment provides the opportunity for learners 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	33	20
Understanding Foreign Ownership, Control or Influence (FOCI)	This course introduced 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	83	1002

Industrial Security Facilities Database (ISFD) Facility Clearance Verification and Notifications for Industry v3	Provides step-by-step instructions on the use of Facility Verification Request (FVR) application feature of the ISFD system to verify the status of a facility clearance	58	974
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	18	12

APPENDIX B - OVERALL PROGRAM ACCOMPLISHMENTS

Since 2008, DoD initiated steps to strengthen and refocus DSS to meet 21st century industrial security and CI needs. Toward this end, DSS enhanced its oversight under the NISP to include an increased focus on CI and security education. During the reporting period, DSS has:

- Performed vulnerabilities assessments of over 8,000 cleared contractors classified security programs. At the end of these assessments DSS issues a rating of the security posture of the facility. To increase standardization and decrease subjectivity of the rating process across the DIB, IO implemented the Security Rating Matrix. The Security Rating Matrix is a numerically based quantifiable approach for DSS to account for all aspects of a facility's involvement in the NISP.

- Conducted a Workload Prioritization Assessment that focused on the value of a contractor's program, seriousness of known threats, and vulnerabilities to security programs. By revamping its threat mitigation strategy and methodology to prioritize assessment-based risk factors, DSS is able to operate ahead of the threat, not behind the vulnerability.

- Started providing industrial security oversight and conducted security vulnerability assessments of cleared U.S. contractor visitor groups accessing classified information on overseas U.S. military installations within the U.S. European Command and U.S. Africa Command areas of responsibility. Due to resource restrictions, DSS is currently limited to providing this oversight via TDY, but despite the limitation, DSS identifies security vulnerabilities at DIB overseas visitor groups and provided industrial security matter expertise to the Combatant Commands.

- Launched a major revision to the DSS database system of record, Industrial Security Facility Database (ISFD), mitigating manual tracking of key metrics on vulnerabilities and deficiencies which can be easily analyzed and shared with industry at key forums to allow them to better focus their resources.

- During FY11, DISCO, which in FY13 became part of the DoD Consolidated CAF, adjudicated 148,696 Intelligence Reform and Terrorism Prevention Act (IRTPA)[8]

[8] The Intelligence Reform and Terrorism Prevention Act (IRTPA) mandated the development of a plan to reduce the length of the personnel security clearance process with the following criteria: to the extent practicable, each authorized adjudicative agency makes a determination on at least 90 percent of all applications for clearances within an average of 60 days from the date of receipt of the completed application. The act states that by December 2009, not more than 40 days should be spent on the investigative phase and not more than 20 days should be spent on the

cases that fell under its jurisdiction.[9] DISCO completed 124,013 adjudicative determinations on initial clearance applications, 90 percent of which were completed within an average of 24.1 days (4.1 days above the 20-day IRTPA goal). DISCO also completed 24,683 adjudication determinations for clearance renewals, 90 percent of which were completed in an average of 28.8 days (well within the 30-day IRTPA goal).

- During FY12, DISCO adjudicated 159,258 IRTPA cases that fell under its jurisdiction.[10] DISCO completed 127,679 adjudicative determinations on initial clearance applications, 90 percent of which were completed within an average of 7.9 days (12.1 days below the 20-day IRTPA goal). DISCO also completed 31,578 adjudication determinations for clearance renewals, 90 percent of which were completed in an average of 8.0 days (greatly exceeding the 30-day IRTPA goal).

- Instituted a Quality Assurance Office (QAO) to assess field processes and procedures, identify inconsistencies or issues, and enhance policy, guidance, training and management support as needed to mitigate any shortcomings. Additionally, this office identifies best practices and ensures they are provided to DSS personnel nationwide.

- Improved NISP C&A timeliness and established a new procedure to mitigate risk to information systems in the hands of cleared industry by reducing timelines for systems operating on IATO. DSS also instituted new procedures for straight to ATOs, in many instances eliminating need for an IATO.

- Signed a Memorandum of Agreement (MOA) [11] that defines the roles, responsibilities, and relationships between Defense Information Systems Agency (DISA) and DSS for contractor classified information systems connecting to the SIPRNET. The MOA establishes DSS inspection teams trained by DISA Field Security Operations to conduct Command Cyber Readiness Inspections (CCRI), at

adjudicative phase.

[9] The cited timelines do not include 11,937 cases that were referred during the reporting period to the Defense Office of Hearings and Appeals for due process determinations or 16,393 cases forwarded to other DoD adjudication facilities for Sensitive Compartmented Information adjudication.

[10] The cited timelines do not include 10,034 cases that were referred during the reporting period to the Defense Office of Hearings and Appeals for due process determinations or 22,104 cases forwarded to other DoD adjudication facilities for Sensitive Compartmented Information adjudication.

[11] DSS CCRI teams are expected to assume CCRIs in the second quarter of FY13. After the transition, DSS will be responsible for NISP contractor SIPRNET CCRIs. There were 148 NISP contractor sites with SIPRNET as of October 2012.

cleared contractor locations where DSS already has oversight responsibilities. This teaming arrangement presents a unified DoD face to defense contractors.

- In 2011, DSS began participating in the Defense Information Assurance Security Accreditation Working Group (DSAWG) meetings in order to advise members and receive information first-hand with regard to government standards that should be levied on cleared contractors. The DSS presence at DSAWG has benefited the NISP significantly and has enabled DSAWG to get immediate answers and input when NISP contract site related issues are raised. The DSAWG includes representatives from the Joint Staff, Department of Defense Chief Information Officer, U.S. Strategic Command (USSTRATCOM), Defense Agencies, DISA, Defense Intelligence Agency (DIA), National Security Administration/Central Security Service (NSA/CSS), United Cross Domain Management Office (UCDMO) and Office of the Director of National Intelligence Chief Information Officer (ODNI CIO). DSAWG supports the Defense Information Systems Network/Global Information Grid (DISN/GIG) Flag Panel in final risk decision authority for DISN (SIPRNET) connections.

- Realigned the Facility Clearance Branch to IO headquarters, streamlining communications and workflow, and performed a full process analysis to improve performance. DSS initiated new tracking mechanisms, identified shortfalls, and updated internal policy and external guidance to streamline facility clearance issuance.

- Improved processes and created assessment plans specifically for facilities under FOCI mitigation agreements or that are freight forwarders for classified information. By tailoring and standardizing assessments for the unique considerations at these types of facilities, DSS ensures even more effective oversight and protection of classified information entrusted to industry.

- Deployed the second annual Voice of Industry Survey of over 13,000 Facility Security Officers to assess their perspective of DSS performance, their partnership with DSS, the biggest threats they perceive, recommendations on how we can continue to improve upon our relationship. The survey results indicate that DSS has clearly improved its support to cleared industry over the past year and the overall relationship is much improved.

- Continued to improve upon and expand the Partnership with Industry Program exchange program. This is a professional development program between DSS and industry security personnel. Cross training DSS and industry security professionals enhances the appreciation for and insight on the effort each undertakes on a daily basis. This program completed its twelfth cycle of exchanges this year with participation from across the country.

- Presented the James S. Cogswell Outstanding Industrial Security Achievement Award to a select group of cleared U.S. contractor facilities (26 in FY12, 17 in FY11) that have maintained the highest standards of protection of our nation's classified material, information and programs, in accordance with the provisions of the National Industrial Security Program.

- Continued to implement cross-regional assessment teams for complex cleared facilities. This approach aids the professional development of the DSS workforce by exposing personnel to facilities and personnel that they would not necessarily have the opportunity to work with in their own geographic regions.

- Stayed focused on optimizing limited resources in FY12. DSS began consolidating Resident Offices within the field, moving personnel from smaller staffed locations to larger field offices. Savings were realized in rents and leases, and performances enhanced with proximity to peers and managers.

- In order to add robustness to the facility clearance process, the FOCI Analytic Division fully implemented a procedure for reviewing every company entering the NISP to ensure all elements of FOCI were properly self-reported. They are currently creating a process allowing for a FOCI review of all NISP companies reporting changed conditions.

- Industrial Policy and Programs created an automated process for the oversight of cleared NISP contractors. The directorate set up a system for constant internet monitoring of sites indicating changed conditions at cleared contractors. All findings are publishing in a weekly document and disseminated to DSS' field elements.

- The FOCI Operations Division (FOD) completed a major restructuring of its division to allow for greater oversight support to larger, more complex companies under foreign ownership and control. FOD action officers have been assigned to foreign parents with significant assets in U.S. cleared industry in efforts to provide subject matter expertise to the oversight of large FOCI companies, their foreign parent and any future acquisitions. In addition, this new structure provides increased support to Industrial Security Field Operations (IO) in assisting with vulnerability assessments and annual meetings with FOCI companies.

- To assist in providing detailed tracking and metric development support, the FOCI Operations Division developed a FOCI case tracking system. This database is the consolidation of several spreadsheets and databases, allowing for greater control over current action officer workload as well as provide for real-time reporting of FOCI actions and metrics.

- During the reporting period, DSS provided input to the DoD CFIUS lead component on more than 200 CFIUS transactions regarding whether the company being acquired had any DSS equities or concerns under its National Industrial Security Program authorities. This includes DSS emplacing FOCI mitigation agreements at 28 companies subsequent to CFIUS approval of the transaction. Furthermore, DSS provided support and subject matter expertise to CFIUS members who have emplaced National Security Agreements as a result of a CFIUS review.

- CDSE successfully hosted its first Learn@Lunch webinar, and due to its success, now offers a new webinar each month. The 30-minute Learn@Lunch sessions have been created in response to the need to provide training for Facility Security Officers (FSOs) and others within industry and government in a format that is accessible and available anytime, anywhere. Approximately 2,154 individuals attended these sessions.

- CDSE has launched several new e-learning courses to include: Understanding Foreign, Ownership, Control or Influence, Security Support to International Industrial Operations, a NISP Certification and Accreditation curriculum, a Virtual Industrial Security Assessment capstone activity, and performance support tools designed for quick reference and/or refresher training.

- CDSE introduced short format learning, known as “Security Shorts.” Recognizing the time demands facing security professionals, CDSE produces training shorts that are usually 10 minutes or less. “Security Shorts” allow security professionals to refresh their knowledge of a critical topic or quickly access information needed to complete a job. The debut of Security Shorts in FY11 was a great success.

- CDSE expanded its Getting Started Seminar for New Facility Security officers (FSOs) to one and a half days. In order to provide the students with the most beneficial learning experience, all of the practical exercises were enhanced and the course curriculum expanded to include lessons on the Security Rating Matrix and the DD Form 254.

- CDSE implemented nine CI awareness e-learning courses online and seven courses with Counterintelligence awareness or threat Briefings.

- In FY12, the DSS CI Directorate identified 657 known/suspected illegal collectors and referred these cases to Federal action agencies.[12]

- Began efforts to build a defensive/preventative cyber security program to include a focus on training with the goal of increasing the cyber security posture in cleared contractor facilities to include the insider threat. Technical cyber training is provided to personnel responsible for information systems as well as to those focused on facilities.

- Cyber threats to the cleared DIB continued their strong upward trend in FY12. To better counter the cyber threat, DSS established a Cyber Operations Division to promote, integrate, focus, and improve DSS' internal performance in cyber and to augment support to its cleared contractor customers.

- Throughout FY12 and FY11, DSS continued to improve and expand its support to the cleared contractor community in confronting the cyber threats to their classified information systems and to U.S. government information residing on unclassified systems within cleared industry which could place classified information and programs at risk. For instance, DSS has developed a number of new products, such as the Cyber Activity Bulletin, which is designed to help cleared industry identify suspicious or possibly malicious cyber activity.

- In FY12, DSS produced 1,678 suspicious contact reports (SCR) that represent one or more discrete cyber incidents occurring on cleared contractors' unclassified systems. This represented a 114 percent increase when compared to the FY11 cyber SCR total of 787. Of those reports, DSS determined that 1,316 had intelligence value, an increase of 186% over FY11. The cyber reporting to DSS and its analysis and subsequent referral to U.S. LE/CI authorities resulted in the opening of 82 investigations, a 37% increase over such actions in FY11.

- In FY12, DSS began personal outreach to the cleared contractors to emphasize the requirement to report suspicious contacts, including cyber incidents. The DSS Field Counterintelligence Specialists (FCIS) visited 601 cleared facilities, of which 286 initiated incident reporting shortly thereafter, and generated 794 suspicious contract reports.

- In FY11, DSS established a cyber threat portal, hosted by the Department of Homeland Security (DHS) on its Homeland Security Information Network

[12] In this context, "Federal action agencies" refers to USG agencies with law enforcement or other operational/National Security authorities to take actions against the referrals transmitted by DSS, including FBI and DHS/Immigration and Customs Enforcement (ICE), and any agency with Title 18 law enforcement or Title 50 National Security authorities.

(HSIN). The DSS portal is available to all cleared contractors to provide access to DSS' unclassified cyber threat alerts and cyber analysis products to assist industry in reducing its cyber-related vulnerabilities and threats. Since it became operational in September 2011, HSIN has grown to over 6,100 cleared contractor accounts.

- In FY12, DSS has also completed production of an online cyber threat awareness course for cleared contractors and DoD personnel which engenders increased reporting from industry by sensitizing contractor personnel within the NISP to cyber threats to their IT systems and resident information. DSS estimates over 15,000 personnel have taken this training since it was implemented.

- In FY12, the Operations Analysis Group (OAG) reviewed, assessed and acted on 590 suspicious contact reports, annual inspection results, counterespionage cases, and Consolidated Adjudication Facility incident reports. The OAG was established to identify individual and systemic vulnerabilities that hinder the effective execution of DSS responsibilities under the NISP. These activities reflect a 375 percent increase from FY10 and resulted in 120 internal and 118 external vulnerabilities identified. Action was taken on 60 personnel security clearances and 4 facility clearances, mitigating previously undetected vulnerabilities within the NISP.