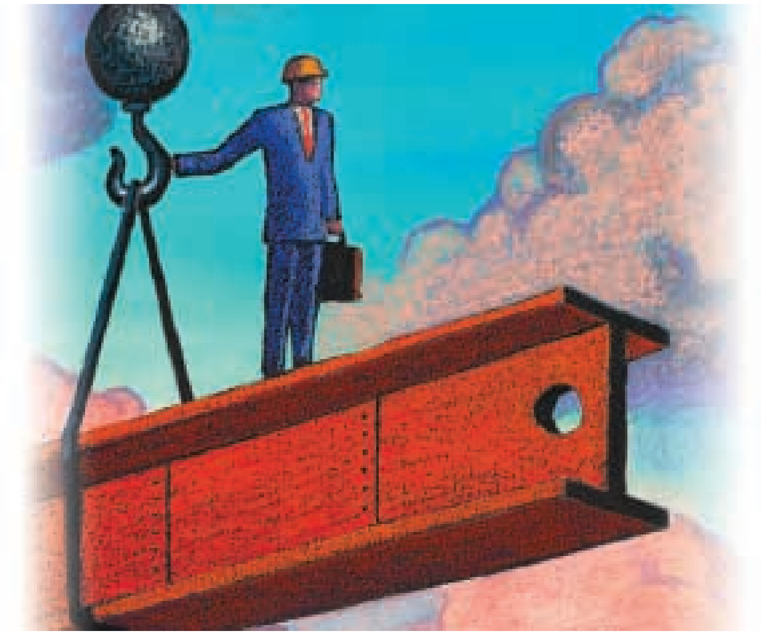
THE 2002 NATIONAL INDUSTRIAL SECURITY PROGRAM REPORT

NISP

THE NATIONAL INDUSTRIAL SECURITY PROGRAM

Industry's Perspective:
Making Progress, But Falling Short of Potential

INFORMATION SECURITY OVERSIGHT OFFICE | ISSUED 2003



"Many thousands of individuals within Government and industry are responsible for the progress made to date in implementing the NISP. There is more that needs to be done and ISOO will be working closely with our partners in industry and Government in building upon a renewed commitment to the NISP's original goals and objectives."

—J. William Leonard
Director, Information Security Oversight Office (ISOO)

CONTENTS

INTRODUCTION

This report provides information on the current status of the National Industrial Security Program (NISP) as part of the Information Security Oversight Office's (ISOO's) responsibilities to implement and monitor the program under Section 102(b) of Executive Order 12829, as amended, "National Industrial Security Program." This is part of our continuing evaluation of Government and industry's efforts to achieve the goal of establishing an integrated and cohesive program that safeguards classified information while preserving the Nation's economic and technological interests.

In keeping with our oversight responsibilities, and in coordination with the Defense Security Service (DSS), and the four NISP signatories—the Department of Defense (DoD), the Central Intelligence Agency (CIA), the Department of Energy (DOE), and the Nuclear Regulatory Commission (NRC), ISOO's NISP team[1] conducted its third review of the NISP over the program's 10-year history. The current survey consisted of an electronic survey of industry representatives, as well as on-site interviews with industry representatives at 52 contractor facilities located throughout the country. The visits allowed the team to meet directly with security representatives to discuss their views and experiences regarding several important aspects of the NISP. More specifically, the visits allowed the team to collect experiential data to determine whether the information collected during the survey represented isolated incidents or a common set of experiences.

We thank the NISP signatories, DSS, and members of the industrial security community who willingly contributed to this effort. We also thank Dr. Dan Lurie, a statistician with the NRC, who lent his knowledge and skill to the project.

[1] See Appendix C for the list of NISP team members.

“Transformation is not an event; it’s a process. It involves a mind set, an attitude, a culture...it involves new ways of thinking, new ways of operating, new ways of doing business.”

—Secretary of Defense Rumsfeld

EXECUTIVE SUMMARY

Executive Order 12829, as amended, “National Industrial Security Program,” (NISP) recognizes the obvious imperative to ensure the proper safeguarding of classified information in the hands of industry. However, what is equally significant is its recognition that our industrial security program must also promote the economic and technological interests of the United States. As such, an essential element of the NISP is its acknowledgment that how the program is implemented is as critical to national security as is the safeguarding of classified information.

Before the creation of the NISP, each agency had its own individual industrial security program. Each program had processes that were unique. The NISP has helped to create an atmosphere of cooperation for both Government and industry by eliminating many duplicative processes. The last review indicated that there was a greater awareness and uniformity in security procedures, increased reciprocal acceptance of personnel and facility security clearances, and increased reciprocal acceptance of agency inspections. Ten years after its inception it would be hard to imagine an environment without the NISP. However, this review has found that, in many respects, the NISP is not meeting its full potential to promote the economic and technological interests of our nation. If measures are not taken to ensure that its full potential is realized, the NISP could undermine many of the “transformation efforts” currently underway in much of the Federal Government. Inevitably, the leveraging of technology and services from the private sector is an integral part of these efforts.

Often, NISP participants refer to the NISP as a “partnership” between Government and industry. However, it is more than that—it is also a legally binding contractual relationship between Government and industry. As with all contracts, both parties commit to do certain things. Industry, of course, agrees to protect classified information by complying with the edicts of the National Industrial Security Program Operating Manual (NISPOM). The Government, in turn, agrees to do certain things as well. In fact, in many instances, Government action is a prerequisite before the contractor can act.

For example, contractors cannot provide an employee with access to classified information until the Government clears that individual. Similarly, oftentimes contractors cannot process classified information on an Automated Information System (AIS) until the Government has approved that system. Likewise, certain areas cannot be used by contractors to safeguard classified information until the Government has approved the area. In the context of ensuring the proper safeguarding of classified information, these prerequisites may appear reasonable. Yet, with respect to promoting the Nation’s economic and technological interests, the Government’s inability to accomplish these prerequisites in a prompt manner or to honor reciprocally a similar action by another Government agency, has a significant and deleterious impact upon cleared industry’s capability.

In essence, as reflected within this report, reluctance on the part of Government agencies to forego some “agency prerogatives” and fully embrace all the tenets of the NISP hampers industry’s ability to recruit and retain the best and the brightest in their disciplines as well as its capability to rapidly develop and field the latest technology when performing on classified contracts in support of its Government customers. As a result of the inability to achieve the NISP’s full potential, contractors are precluded from putting forth the best conceivable efforts in both cost and capability in supporting their Government customers’ current transformation efforts. As such, the Government effectively gets less for more.

This report calls for a renewed commitment by Government to the NISP’s original goals. Such a commitment would help address the main concerns expressed by industry as set forth in this report.

Chief among the concerns expressed in this survey were:

- **Slow processing of personnel security clearances:** Despite reworking the personnel security clearance process several times, industry is still reporting cases that take several years to be processed.
- **Limited reciprocity in regard to facility and personnel security clearances:** Government employees still have more flexibility when dealing with clearances and reciprocity than industry employees have despite repeated discussions to resolve the issues.
- **NISPOM guidance remains inadequate for some:** Many in industry, especially those new to the program, express frustration with vague guidance.
- **Rewrite of Chapter 8 has improved the processing of classified information on Automated Information Systems, but it does not fully meet the needs of industry:** Industry is asking for more detailed guidance on how to design their AIS and write the system plans for accreditation.
- **Threat information is timely but needs to be more relevant:** Survey participants, overwhelmingly, report that the information they receive is not seen as relevant and applicable to their situations. Additionally, many in industry feel that too much emphasis is placed on the external threat, when in many instances the real threat is cleared personnel.
- **No uniform instruction for the handling of Sensitive But Unclassified (SBU) information creates confusion for the end user:** Different agencies use different language for what is essentially the same information, and this causes confusion for industry when dealing with multiple agencies.

Solutions

In order to better focus and coordinate industry and Government's efforts with respect to implementation of the NISP it is essential for ISOO to standup to its role as originally envisioned in E.O. 12829, as amended. Specifically, ISOO shall:

1. require that all executive branch agencies that are participants in the NISP submit their implementing regulations, internal rules, or guidelines pursuant to E.O. 12829, as amended, Sec. 102(b)(3) by August 15, 2003;
2. pursuant to E.O. 12829, as amended, Sec. 102(b)(1), develop by December 31, 2003, in consultation with the agencies, a draft final directive for implementation of this Order. Following subsequent formal coordination and promulgation, subject to approval of the National Security Council, this directive shall be binding on the agencies;
3. conduct on-site reviews of the implementation of the NISP by each agency, contractor, licensee, and grantee that has access to or stores classified information and to require of each agency, contractor, licensee, and grantee those reports, information, and other cooperation that may be necessary to fulfill the Director of ISOO's responsibilities pursuant to E.O. 12829, as amended, Sec. 102(b)(4); and,
4. host Town Hall meetings to continue the dialog between Government and industry on prevailing issues.

a single, integrated,
cohesive system

I. BACKGROUND

Executive Order 12829, as amended, “National Industrial Security Program,” (NISP) recognizes the obvious imperative to ensure that classified information in the hands of industry is properly safeguarded. However, what is equally significant is its recognition that our industrial security program must also promote the economic and technological interests of the United States. As such, an essential element of the NISP is its acknowledgment that redundant, overlapping, or unnecessary requirements imposed upon industry can imperil national security as readily as can the improper safeguarding of classified information.

Pursuant to E.O. 12829, as amended, there are four signatories to the National Industrial Security Program: the Department of Defense (DoD), the Central Intelligence Agency (CIA), Department of Energy (DOE), and the Nuclear Regulatory Commission (NRC). In addition, all other Federal agencies that engage contractors on a classified basis are required to assume the status of User Agencies.

E.O. 12829, as amended, assigns operational oversight of the NISP to the Secretary of Defense, who acts as the Executive Agent for the NISP and has final responsibility for issuing and maintaining the National Industrial Security Program Operating Manual (NISPOM). The NISPOM serves as the single regulatory standard for industry.

The Executive Agent also provides cost information through the Information Security Oversight Office (ISOO) to the President on the implementation of the NISP. The Director of the Defense Security Service (DSS) administers the NISP on behalf of the Secretary of Defense and User Agencies. In conjunction with these responsibilities, the Director of DSS is responsible for the administration of the Industrial Security Program for DoD and 24 non-DoD User Departments and Agencies of the Executive Branch, which are signatories to an agreement with DoD.

According to the Order, the Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information (SCI). Likewise, both the Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

E.O. 12829, as amended, requires that ISOO implement and monitor the NISP and oversee agency, contractor, licensee, and grantee actions in order to ensure that they comply with the Order. ISOO is also required to review all agency implementing regulations, internal rules or guidelines, and conduct periodic on-site reviews of the implementation of the NISP by each agency, contractor, licensee, and grantee that has access to or stores classified information. Additionally, the ISOO Director serves as Chair of the National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC advises the Director on all matters concerning the policies of the NISP, including recommending changes to those policies. The NISPPAC also serves as a forum for discussing policy issues in dispute.

II. SURVEY GOALS AND METHODOLOGY

In keeping with its responsibilities, ISOO continues to evaluate the effectiveness of the NISP in establishing an integrated and cohesive program that safeguards classified information while preserving the Nation's economic and technological interests. The objectives of ISOO's recent assessment were to: 1) evaluate adherence to program goals and objectives; 2) assess industry's perceptions and attitudes toward the NISP; 3) identify systemic problems; and, 4) provide solutions.

As in prior reviews, ISOO chose contractors to reflect a mix of various sized companies with classified holdings. The NISP team met with the Security Directors of the major signatories to the NISP. The team also met with DSS to solicit its support and obtain a listing of its Government contractors by size and holdings. These holdings include collateral Classified National Security Information, Restricted Data and Formerly Restricted Data, SCI, and Special Access Program information.

While there are similarities between this assessment and previous ones, there are some differences. This assessment is broader in scope and methodology. Instead of randomly choosing contractors to participate, ISOO sent out a survey electronically to all contractors in the DSS system that have the capability to possess classified information, in much the same way that the Office of the Secretary of Defense fulfills its annual requirement to collect cost data for the NISP. ISOO augmented the DSS list with facilities unique to the CIA and DOE. Therefore, the survey was sent to 4,709 contractors. We also contacted NRC, but could not include the one contractor on its list in time for the online part of our assessment.

The survey began on August 15, 2002, with DSS providing an email link for contractors to the online survey. The survey ended on September 13, 2002. In order to facilitate a candid exchange of information, ISOO assured respondents that their personal and company names would be kept confidential. ISOO gathered the data and analyzed it in several ways. First, the original data was separated into five groups that corresponded to the geographical region that each respondent reported in the survey. In writing the survey, ISOO used the same five geographical regions that DSS uses in their industrial security program. Secondly, the original data was separated into four categories of facility size. These categories were based on the number of cleared employees at each facility that the survey respondents reported. ISOO then ensured that all regions and categories of size were well represented and the team analyzed the collected data using statistical procedures.[2] Finally, the data was separated by Cognizant Security Agencies (CSA) to give an overview of differences in agency programs, but a full statistical analysis was not performed on these data.

To underscore the importance of the survey, validate the findings, and enrich the data obtained, ISOO supplemented the survey with on-site interviews across the United States. The site visits, which consisted of a variety of contractors, based on size and holdings, began on October 20, 2002, and ended on January 30, 2003. They involved 52 contractor facilities in the following areas: San Diego, California; Albuquerque, New Mexico; Huntsville, Alabama; Red Bank, New Jersey; King of Prussia, Pennsylvania; and the Washington, DC, metropolitan area. ISOO used 13 set questions[3] at each facility. In addition, the analysts asked additional followup questions where more elaboration was necessary. ISOO sent at least two analysts to each facility to conduct interviews, and each interviewer compiled his or her own set of notes. After completing the interviews, the analysts compared, discussed, and compiled their notes for use in this report.

The site visits were beneficial because they allowed the NISP team to meet directly with Facility Security Officers (FSOs) and other corporate security representatives to discuss their views and experiences. More specifically, the visits permitted ISOO to collect experiential data to determine whether the information collected during the survey represented a common set of experiences or isolated incidents.

After completing a draft report, ISOO contacted the four CSAs, as well as DSS, and provided a copy of the draft to them for review and comment.

[2] Samples of the statistical results are in Appendix E.

[3] A copy of the on-site interview questions can be found in Appendix B.

III. STATISTICAL METHODS

ISOO applied standardized statistical methods and procedures to data collected on a relatively small scale to form logical conclusions about the general case. Our survey consisted of 52 questions of which 31 were amenable to analysis. Not all of the 31 questions that ISOO analyzed provided useful and relevant data, and, as such, not all are contained within the body of this report. Of the questions analyzed, 28 were binary or "yes/no" questions, and three were multiple-choice questions. For each question, a chart was created to show the statistical breakdown of the classification variables—region and size.[4] Appendix A provides the questions from the survey.

In conducting the analysis, several assumptions were made, including the following:

1. All facilities received the questionnaire announcement in a timely manner.
2. All facilities that received the questionnaire believed that personal and company names would be kept in confidence.
3. All facilities had equal access to the Internet, resources and time allowance, as well as an equal opportunity to complete the questionnaire.
4. The sample is representative of the population—those who did not respond are the same as those who did, and their answers would not be appreciably different from the sample.
5. The 393 who responded represent the entire population and the issues and/or problems that these 393 facilities brought forth are representative of the entire population's issues and/or problems.

By incorporating statistical methods in analyzing the data, the NISP team drew conclusions from the data to give a clear picture of the NISP in its present state. To ensure the use of proper methods and procedures, ISOO consulted with Dr. Dan Lurie, a statistician with the NRC, who lent his knowledge and skill to the project for several months and aided in the interpretation and validation of the survey results. In this regard, it's important to note that this survey did not expect to receive questionnaire returns from all companies. However, it was intended to receive a random collection of responses from the participating pool of facilities. The design of the survey, as expressed in the stated assumptions in the "Statistics" section, has followed the steps required for a random sample. Departures from randomness are inherent in almost any survey due to the individual bias, mood, and perspective of the respondents, and this survey is no exception. Consequently, any percentages and confidence intervals presented in this analysis may be somewhat distorted from the truth, but are not necessarily biased. To assure the reader that these numbers are not carved in stone, we provided in the confidence interval(s) an understandable measure of variability, even if it is not exact.

ISOO first analyzed the data in their completed state to give an overall view of the NISP. The statistical analysis determined that the data sample of 393 responses was of sufficient size and form to allow ISOO to perform both upper and lower confidence levels at the 95 percent level.[5] The 393 responses in the sample were then stratified to allow us to test whether a pattern of response could be associated with a geographical location or correlated with the company size and number of cleared employees in a given facility. Figures 1 and 2, respectively, show a breakdown of the population and sample by size and region.

Figure 1 shows that, in the Capital region, the percentage of responding companies is considerably lower than other regions. There is no compelling explanation for this low rate of participation. Figure 2 shows that the survey response rate is proportional to the company size. In other words, as the size of a facility increases there is a greater likelihood that the company will respond to the survey. There is no definitive explanation, but one possible explanation is that larger companies have more resources and were better equipped to respond to ISOO's voluntary request for participation in the survey.

ISOO conducted statistical analyses to investigate whether companies across strata (geographic regions or company size) were responding alike. By separating the data and analyzing them in this way, systemic strengths and weaknesses of the NISP could be located and tracked across strata.

During the statistical analysis of the online survey, the data were broken down into five categories that correspond to the geographical regions that DSS uses in their industrial security program. The five regions that DSS uses are the Western, Central, Southeastern, Capital, and Northeastern regions.

[4] For more information on this and for copies of the analysis, please contact ISOO at *nisp@nara.gov*.

[5] Confidence limits are not included in this report, but may be obtained by contacting ISOO.

Figure 1: Population and Sample by Region

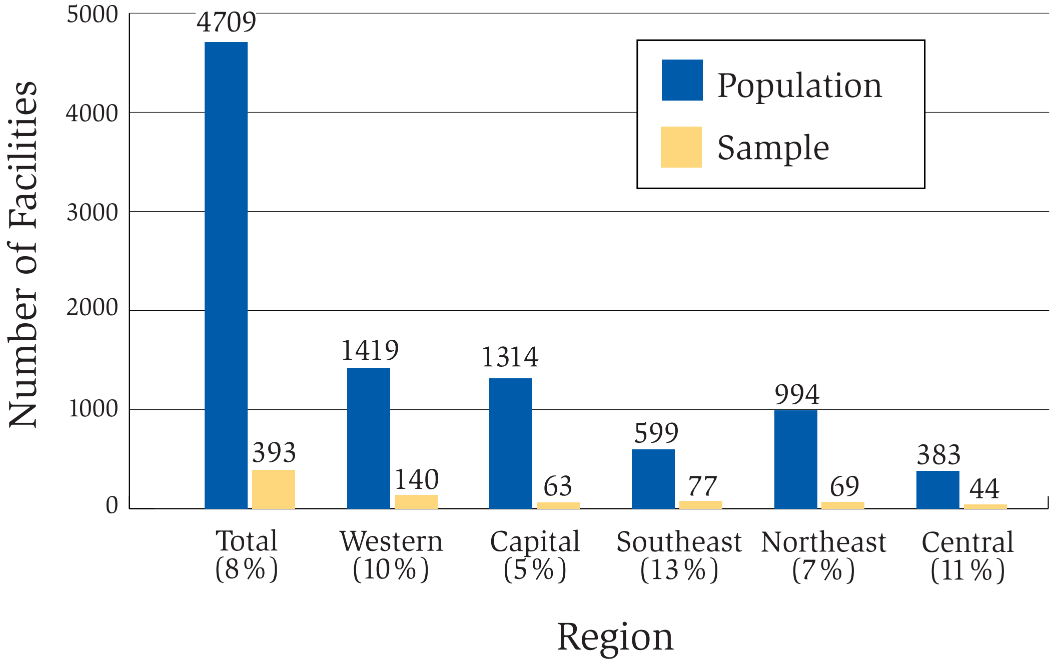
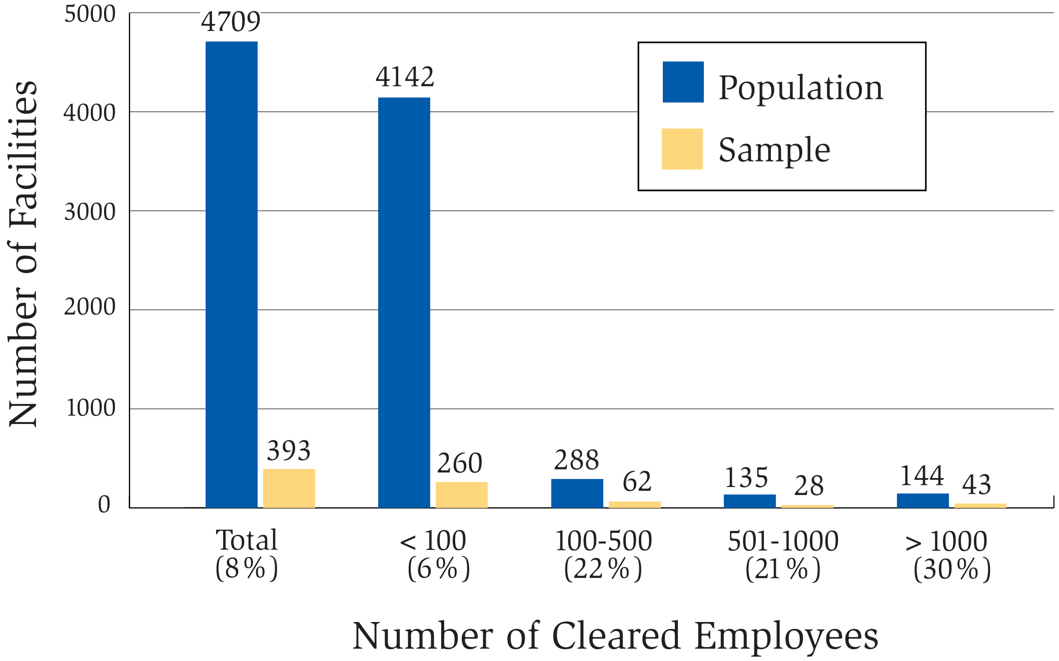


Figure 2: Population and Sample by Number of Cleared Employees



This analysis was conducted to see if there were any regional disparities in responses. ISOO could not discern any definitive patterns from the analysis and it appears that all regions, with the exception of the Capital region, responded similarly to the survey. In many areas the Capital region appeared to show slightly higher levels of dissatisfaction and increased levels of concern in their responses, but these levels were not high enough to draw definitive conclusions on the level of dissatisfaction in the Capital region compared to the rest of the country.

The data were also broken down into four categories by size and analyzed. This analysis was conducted to see if there were any varying levels of concern based on the size of facilities. Each category represented the number of cleared personnel that are employed by the responding facilities. The analysis revealed that in many cases the concerns of the smaller (less than 100 cleared employees) and those of the largest (more than 1,000 cleared employees) differed by a substantial statistical amount, showing that there are significant differences in the levels of concern experienced by smaller facilities when compared to the concerns of larger facilities.

Finally, ISOO separated the survey results based upon whether the respondent reported performing on DoD, CIA[6], and/or DOE contracts. Due to overlapping data sets, statistical analyses were not performed on these data, but they were reviewed in order to give the assessment team a better appreciation of problems industry encounters when working with each of the four CSAs. Where percentages for CIA and DOE are included in this report, they are not alluding to any statistical methods or data. However, they mirror the information gathered at the interviews and, therefore, serve as an indicator of the high levels of concern and the seriousness of these concerns. While separating the data by CSA does not give a full picture of problems present at each individual CSA, it does provide an outline that was comparable to the information presented during on-site interviews.

This report represents a synthesis of the data collected from ISOO's survey with data that ISOO gathered during interviews with facility personnel during site visits. All recorded percentages represent responses to the survey and should be viewed as such. Because of the empirical nature of the data collected during the on-site interviews, there are no statistical data or percentages to present. However, the experiences expressed to ISOO are captured and reported in the body of this report. Where possible, credible reasons are provided to explain cases where a disparity existed between the data collected in the online survey and data collected during interviews. If no reasonable explanation for inconsistencies was identified, then the data are reported as collected, without explanation.

[6] The information provided to ISOO, by the CIA, for facilities with CIA contracts did not allow a separation of facilities by SCI and collateral contracts. ISOO analyzed all CIA contracts as being the same with no distinction between CIA's SCI and collateral programs.

IV. FINDINGS

Overall, this report reveals that items identified as progress points in our January 1999 NISP report are no longer progressing. Our 1999 survey revealed substantial uniformity in security procedures and increased reciprocal acceptance of personnel and facility security clearances. However, our 2002 survey and on-site interviews reveal a significant weakening in these same areas. Nonetheless, according to responses from industry, the four NISP CSAs have not manifested this weakening to the same degree. Of the three NISP signatories[7] that participated in the survey (DoD, CIA, and DOE), DoD contractors were more positive in their comments in both the online survey and the on-site interviews.

This review has found that, in many respects, as currently administered by the Government, the NISP is not currently reaching its full potential to promote the economic and technological interests of our nation.

A. Industry's Perceptions and Attitudes

Achieving Goals and Objectives: In terms of both a strength and weakness, it is very encouraging to report that 90 percent of all respondents to the online survey actually view the NISP/NISPOM positively in terms of achieving its overall goals and objectives. However, this overall positive result falls off significantly when focusing on those respondents who reported that they were working on DOE and/or CIA contracts. Specifically, it appears that roughly 60 percent of the respondents with CIA contracts[8] and less than 40 percent of the respondents with DOE contracts[9] feel that the NISP is achieving its goals and objectives.

Quality and Timeliness of Guidance: Ninety-four percent of the respondents to the online survey rated positively the guidance they receive from their CSAs with respect to the NISP and the NISPOM. DOE and CIA contractors provided less positive assessments when comparing their responses to the entire population. Roughly, 65 percent of the survey respondents with CIA contracts and around 50 percent of the respondents with DOE contracts rated the guidance they receive positively.

Guidance With Respect to Points of Contact: The respondents indicated that they are provided clear guidance with respect to whom they should contact when in need of assistance with the NISPOM or other industrial security guidance. Only 10 percent of all survey responding facilities that have DoD contracts reported that they do not receive adequate program reviews to assess security vulnerabilities. Taking together on-site interviews and the survey data, this shows that within the DoD community there appears to be a strong framework for information sharing, assistance, and assessment services to industry. In contrast, around 30 percent of all respondents that have CIA contracts and roughly 45 percent of all respondents that have DOE contracts do not believe that they are receiving adequate program reviews. Taking together on-site interviews and the survey data, this indicates that, within the CIA and DOE community, many respondents believe that they are not getting the attention and assistance that they need.

> It appears that roughly 60 percent of the respondents with CIA contracts and less than 40 percent of the respondents with DOE contracts feel that the NISP is achieving its goals and objectives.

Overall Awareness and Quality: More than 80 percent of all facilities that replied to the survey are aware of the NISP. Over 75 percent of respondents have also seen improvements in the NISP since its inception. Among the other 25 percent who responded to the survey, many noted that they were new FSOs and lacked historical perspective to see any change in the NISP.

General Comments: The results of the survey and interviews revealed industry's sweeping endorsement of the Electronic Personnel Security Questionnaire (EPSQ). The EPSQ is the electronic version of the Standard Form 86, "Questionnaire for National Security Positions," which allows the user

[7] See "Survey Goals and Methodology" section of the Report (Page 5).

[8] Of the 393 respondents to the survey, 50 claimed CIA as their CSA or claimed to have another agency as their CSA, but have contracts with CIA.

[9] Of the 393 respondents to the survey, 54 claimed DOE as their CSA or claimed to have another agency as their CSA, but have contracts with DOE.

to complete the application process for personnel security investigations electronically. According to the participants, the EPSQ has made "doing business" with the Federal Government much easier. With the EPSQ, they noted a significant improvement in their ability to update, remove, or reinstate the clearance information for individuals within the company who are either new hires or departing employees. Other enhancements to the NISP that were mentioned include: (1) DoD interim clearances, which were granted under most circumstances in a timely manner; and (2) the ability to use "waivers" at certain agencies, which allows security personnel the capability to move individuals around without unnecessary "red tape."

B. Perceived Systemic Problems

1. Slow Processing of Personnel Security Clearances

Roughly, 45 percent of the facilities with DoD contracts that responded to the survey have concerns regarding the granting of personnel security clearances. As reported in June 2003, at the National Classification Management Society's Annual Training Seminar, as of May 30, 2003, there were over 424,580 cases in the DSS and Office of Personnel Management's combined backlog. According to DSS, the ideal situation would entail a combined total of 150,000 cases.

For contractors with CIA and DOE contracts, there are even greater levels of concern. Around 60 percent of the facilities with CIA contracts and 70 percent of the facilities with DOE contracts reported that they have concerns with the granting of personnel security clearances. The main concerns expressed by these contractors did not center on any backlogs, but on the overall length of time it takes their employees to receive clearances. DOE reports that they do not have a backlog at this time, but their contractors still express frustration with the amount of time it takes to process clearances and the fact that certain DOE labs require additional paperwork for internal administrative processes that the labs have implemented.

> *A Contractor's Perspective*[10]:
>
> " Working with DOE and DoD, I have found that DOE produces their own orders and directives, and DoD adheres to the NISP. "

The on-site visits confirmed the concerns mentioned above. The principal concern expressed was the length of time it takes to process the clearances. As of May 2003, there were 18,515 cases in the DSS backlog that were between 271 and 360 days old and 27,253 cases that were over 360 days old.

According to those interviewed, the delays cost industry countless millions of dollars per year. They indicated that the delays also affect personnel resources. Specifically, those interviewed reported difficulty in filling sensitive positions and retaining qualified personnel. Often individuals left the company before they actually worked in the position they were hired for, due to delays in the clearance process. From the perspective of those interviewed, the delays hamper their ability to perform duties required by their contracts, thereby limiting their ability to perform a valuable service to the United States Government.

2. Limited Reciprocity with Facility and Personnel Security Clearances

Reciprocity is a major tenet of the NISP. Reciprocity involves the acceptance of one agency's certification by another agency without additional requirements.

a. Personnel Security Clearances

The results of the survey and the site visits revealed that the majority of the respondents either had experienced or are currently experiencing problems with reciprocity concerning personnel security clearances. Based upon the responses given, it is difficult to recognize that the entire executive branch is supposed to be operating under uniform investigative standards and adjudicative guidelines for security clearances. On the one hand, throughout most of DoD reciprocity appears to be working. Interviewees stated that when a person moves from one DoD facility to another, the personnel clearance moves with little or no trouble, and neither the agency nor the person who requested the transfer needs new paperwork. Due to the system implemented by the Defense Industrial Security Clearance Office (DISCO), a person's clearance can be readily checked and transferred to a new location. Conversely, according to those interviewed, the same cannot be said for transferring clearances to agencies such as the CIA, the National Security Agency (NSA), or DOE. The interviewees stated that an individual requesting a clearance needs to fill out new paperwork and must reportedly wait an average of three to six months for the personnel clearance to be processed or verified before they can start work on their contract. Furthermore, it was reported that DOE will not accept an electronic version of the EPSQ or printed applications from DSS. Overall, the interviewees expressed frustration with having an employee who has a clearance, but CIA or DOE does not recognize it in all cases. According to the interviewees, these cleared personnel cannot do their jobs, and ultimately, companies incur exorbitant costs because their

[10] *A Contractor's Perspective* quotes were taken from responses to the electronic survey.

employees cannot perform the duties for which they were hired.

Another concern expressed was that DOE and some of the intelligence agencies have their own forms for processing clearance actions. Consequently, according to those surveyed and interviewed, it is not uncommon for DOE to require a second set of paperwork from a DoD facility even though DOE is aware that a periodic reinvestigation is in process. This is an example of a waste of valuable resources and an unnecessary duplication of the investigative process, which is not permissible according to Section 2-200e of the NISPOM. Furthermore, it undermines the intent and spirit of the NISP, which is to achieve a single, integrated, and effective industrial security program.

b. Facility Security Clearances

Only 74 percent of the survey respondents reported that the reciprocity principle for facility clearances is being applied. This finding was also reported by those interviewed during the site visits. A significant number of companies with multiple agency contracts indicated instances when reciprocity was not working. During the site visits, those companies with multiple contracts cited instances of agencies using their own sets of requirements, regulations, and paperwork as the reason for the problem.

As an example of the above, many of those surveyed indicated that DOE facilities operate independently of one another and that each DOE facility has its own separate and distinct procedures for handling facility clearances and clearance verifications. Additionally, the survey and the interviews indicated that DOE does not accept personnel or facility clearances from other CSAs. From the perspective of many of those surveyed and interviewed, DOE operates outside of the NISP framework.

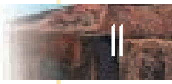
3. NISPOM Guidance Remains Inadequate for Some

Before the creation of the NISPOM, all contractors relied on the Industrial Security Manual for Safeguarding Classified Information (ISM), circa 1991. The ISM provided prescriptive or specific guidance. Conversely, the NISPOM was written to be less detailed and more risk-based. However, for many of the smaller companies and some of the larger companies, particularly those with an influx of new security personnel, the NISPOM is too vague and does not provide enough definitive guidance. This is a significant finding given that the majority of the companies involved in the NISP are small.

In ISOO's January 1999 NISP Report, our first recommendation was that the Executive Agent develop more prescriptive based handbook(s) for requirements of the NISPOM to provide an option to smaller contractors who need more detailed procedural guidance. This recommendation was not implemented. Programmatically, this has had a considerable impact on the overall effectiveness and efficiency of the NISP. Specifically, the ambiguity in the NISPOM has forced many of the more experienced FSOs to continue relying on the ISM for its detailed guidance, while the newer FSOs, who came after the ISM was replaced by the NISPOM, are exceedingly reliant upon their DSS representatives for guidance and assistance. Some respondents to the survey stated that they received conflicting guidance from different DSS representatives or have difficulty reaching their DSS representatives. Thus, excessive reliance on the representative's guidance can reduce the effectiveness of FSOs. When FSOs are unsure of the proper policies and procedures to implement, there is an increased likelihood that classified information may be mishandled or that security safeguards over and above the requirement may be needlessly imposed.

A Contractor's Perspective:

> "...we need more coordination/reciprocity between DoD and DOE facilities..."



4. The Rewrite of Chapter 8 Has Improved the Processing of Classified Information on Automated Information Systems, but does not fully meet the Needs of Industry

Chapter 8 of the NISPOM describes the minimum security requirements for AIS processing of classified information as prescribed by DoD. Eighty-one percent of those surveyed replied that "yes" the new Chapter 8 adequately addresses AIS, but in the followup question, which asked for an explanation for any problems that facilities have with Chapter 8, a majority of the respondents gave examples of problems that they have experienced in implementing Chapter 8 at their facilities. The results show that Chapter 8 addresses many pertinent topics, but contractors are still having problems getting their systems accredited in a timely fashion, based on their implementation of the guidance.

There were additional concerns as well:

- Chapter 8 does not provide explicit guidance. From the perspective of the majority of those interviewed, the guidance is ambiguous and vague and does not clearly indicate how to implement the Chapter. Many facilities, especially small facilities, do not have a full-time Information Systems Security Manager (ISSM)

A Contractor's Perspective:

> "Being from a small company, just learning the process can be quite overwhelming and cumbersome..."

and, therefore, have difficulty fulfilling the duties associated with an ISSM. They view the language in Chapter 8 as a major obstacle. They believe that if they better understood the language it would be easier to write the required System Security Plan (SSP).

- Many DSS Information Systems Security Representatives (ISSRs) are not uniformly implementing Chapter 8 from region to region. Many companies expressed frustration when DSS accredited a SSP in one region but DSS deemed a replica of that system's SSP to be inadequate in another region.
- From the perspective of many Government and industry personnel interviewed there are apparently not enough personnel to handle all of the system accreditations that industry requires. At several public meetings and conferences, industry has stated that, until recently, the DSS ISSRs did not have the training to address their more complex issues or provide consistent advice from region to region on how to develop their system plans. Now that they have received concrete guidance, many feel it is too late. DSS reports that it has been working to solve these problems, but many question if it is enough to avert problems resulting from an upcoming deadline.
- All contractors that receive services from DSS must have their AISs accredited by May 1, 2004. All systems that are not accredited by this date will be shut off, and processing of classified will not be allowed until the systems are accredited. According to industry, many fear that the systems they have been using for the past year under interim accreditations will be shut off because DSS does not have the ability to accredit their systems in a timely manner. Many feel that they will be punished for the inadequacies of DSS's program.

Classified information is at greater risk when in an AIS environment. Given the increased use and reliance on AISs to generate and process classified information, we need to make certain that the proper measures are taken to implement and secure such systems in a timely manner before work of a sensitive nature is performed. To ensure that industry has the tools required to perform the work it was contracted to perform, Government is obligated to make certain that the guidance provided is accurate, timely, and that industry is readily able to implement it.

Some interviewees stated that if they must wait and expend resources while waiting for an AIS to be accredited before working on their contracts, they cannot meet their full potential in terms of timeliness and cost in fulfilling their Government classified contracts.

5. Prescriptive Guidance Does Work

From industry's perspective, the "Florida Plan," as it is most commonly known within the industrial security community, is an excellent example of how the requirements of Chapter 8 of the NISPOM can be uniformly addressed. In order to alleviate the ambiguity of network security plans (NSP), the Florida Automated Information Systems Security Representative Council of the Central Florida Industrial Security Awareness Council (CFISAC) designed and developed several samples of baseline electronic NSPs. Each template was created so that it might be easily modified based upon the needs of the contractor. The NISP team learned that these templates are readily available through the CFISAC web site[11] and that various industrial security awareness groups across the country are using them. The templates were created with the expressed purpose of assisting industry in meeting the requirements outlined in Chapter 8 of the NISPOM. The development and execution of these plans exhibit industry's willingness to comply with the NISPOM. *If implemented and used correctly these plans can serve as an example of how Chapter 8 can be adapted into a useable format for implementation community-wide.*

During conversations with the CSAs, the NISP team learned that the CIA and DSS were jointly working on a project to bring prescriptive guidance to assist industry in writing system plans for AIS. The CIA is creating the Feedback and Automated Systems Security Plan Template (FAST). Though this template is being created by CIA, CIA is sharing its work with DSS to ensure that the template, and the language used in it, will be easily understood by those with CIA as their CSA, as well as those with DoD as their CSA. This electronic template is a prime example of a joint initiative undertaken by the CSAs to meet a need in industry.

6. Threat Information Is Timely But Needs to Be More Relevant

In light of the current threats to our national security, the NISP team believed it was important to see how well contractors were being informed by their CSAs on how to address or identify a viable threat to a current program or a facility even if this area is not specifically covered by the NISPOM. Through the NISP survey, we approached this matter, by asking: (1) whether contractors have been successful in obtaining timely threat information from their CSA or another Government source; and (2) do they believe they have received an adequate review of their security programs in light of those threats.

In response to the first question—whether they have been successful in obtaining timely threat

[11] http://www.cfisac.org/ais.htm

information from their CSA or another Government source—the overwhelming majority of the respondents to the survey believed they received timely threat information. Many of those who responded favorably to this question indicated that they obtained threat information electronically from the FBI's Awareness of National Security Issues and Response program, more commonly known as ANSIR. They also receive information from their contacts within industry and at National Classification Management Society meetings or their local Industrial Security Awareness Councils.

While a majority in the survey indicated that the information they received was timely, many of them were not as satisfied with the quality of the information they received. Specifically, they stated that the information they received was of a general nature. What they would prefer is program specific threat information. The opposite position was taken by those interviewed. They were quite satisfied with the assessments provided.

To a much smaller degree, the electronic survey revealed that a number of contractors lacked knowledge as to what a threat is and how it relates to them. Several of the respondents indicated that because of their size or remote location they did not have any threats.

In fiscal year 2002, the number of suspicious contact reports received by DSS from cleared defense industry was up 86 percent over the previous year. DSS is projecting that the numbers from fiscal year 2003 will be 46 percent higher than those for 2002. These numbers show that the perceived threat has increased substantially and greater emphasis on the education and training of industry is needed to ensure that industry is aware of correct procedures for identifying, taking action against, and reporting any perceived threats.

In response to the second question—approximately 90 percent of the respondents indicate that they currently receive adequate program reviews from their CSAs to assess security vulnerabilities. According to the data from the survey and the on-site interviews, from industry's perspective, the current reviews are adequate. They have not been bolstered as a result of 9/11, nor do they need to be.

7. Lack of Uniform Instructions for the Handling of Sensitive But Unclassified Information (SBU) Creates Confusion for the End User

Although outside the scope of E.O. 12829, as amended, and the NISPOM, a pronounced problem today, consistently identified by many industry representatives through both the survey and on-site interviews, is the lack of uniform instructions for the handling of SBU information. The use of various terms to identify information that is considered unclassified but sensitive continues to be a frustration for industry. For classified information, most Government agencies have long established guidelines governing what information should be classified and safeguarded. The same cannot be said for SBU information.

A Contractor's Perspective:

"The word '***Sensitive***' is being misapplied every day...."

According to the electronic survey analysis, 60 percent of the respondents indicated that they believe they have inadequate guidance with respect to the handling and identification of SBU information. According to our analysis, CSAs, involved in the survey, are not "speaking" the same language and are applying different protection standards for the same information. A major concern for those who were interviewed is how this type of material should be identified. For example, DOE identifies SBU information as Official Use Only or "OUO" information. State identifies it as "SBU" and formerly called it Limited Official Use or "LOU." Similarly, DoD identifies the information as For Official Use Only or "FOUO." For DoD, "FOUO" material may be released to officials in other departments and agencies of the executive and judicial branches for the performance of a valid Government function. According to the DOE guidance, "official use only" information may be disseminated only to those persons who require it to conduct official business, and who have a need-to-know. The various designations refer to unclassified, sensitive information that is or may be exempt from public release under the Freedom of Information Act.

Again, a major problem is caused by the fact that there is not one set of guidelines. Under the current circumstances, it is difficult to determine what is important and what is not. For companies that work with multiple agencies, it is particularly difficult to determine how to handle the sensitive information that does not fall under the rubric of E.O. 12829, as amended, since there is no specific handling guidance.[12]

[12] See pages 33 and 34 for additional clarity.

V. SOLUTIONS

In order to better focus and coordinate industry and Government’s efforts with respect to implementation of the NISP, it is essential for ISOO to stand-up to its role as originally envisioned in E.O. 12829, as amended. Specifically, ISOO shall:

1. require that all executive branch agencies that are participants in the NISP submit their implementing regulations, internal rules, or guidelines to ISOO pursuant to E.O. 12829, as amended, Sec. 102(b)(3) by August 15, 2003;

2. pursuant to E.O. 12829, as amended, Sec. 102(b)(1), develop by December 31, 2003, in consultation with the agencies, a draft final directive for implementation of this Order. Following subsequent formal coordination and promulgation, subject to approval of the National Security Council, this directive shall be binding on the agencies;

3. ensure timely implementation through the conduct of on-site reviews of the implementation of the NISP by each agency, contractor, licensee, and grantee that has access to or stores classified information and require of each agency, contractor, licensee, and grantee those reports, information, and other cooperation that may be necessary to fulfill the Director of ISOO’s responsibilities pursuant to E.O. 12829, as amended Sec. 102(b)(4); and,

4. host Town Hall meetings. On June 11, 2003, ISOO’s NISP team hosted its first Town Hall Meeting at the National Classification Management Society Conference in Salt Lake City, Utah. Representatives from DSS, DoD, CIA, and DOE served as panelists for this meeting. Audience members posed questions to representatives from these agencies and prompted the agency representatives to share and discuss current initiatives underway within their respective agencies. Feedback from the workshop was favorable, with comments such as, “Excellent method of getting out current information, and expressing comments on what is working, what needs fixing or needs to be looked at,” to “very useful to understand why things happen the way they do.” Most importantly, participants felt that more forums of this nature would be beneficial. ISOO is currently planning additional regional “Town Hall Meetings” in the near future.

VI. APPENDIXES

APPENDIX A
SURVEY QUESTIONS

NISP Survey

Please provide the following information.

TITLE

COMPANY

ADDRESS

CITY STATE OR PROVINCE POSTAL CODE

PHONE FAX

EMAIL

COUNTRY

NISP MEMBER'S DSS CAGE NUMBER

Background Information

This information is collected to determine the general statistics for facilities—by size, customer, and location. We will also ask questions about your experience as the security representative and your familiarity with various industrial security initiatives associated with the National Industrial Security Program (NISP).

1. How long have you, as an individual, worked with the National Industrial Security Program?

(Select only one.)

□ Less than one year.
□ One to five years.
□ Five to seven years.
□ Seven to ten years.
□ More than ten years.

2. Please check the box that corresponds to the region where your facility is located.

(Select only one.)

□ Central (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska,
□ Capital (Maryland (Central and Southern) Northern Virginia and Washington DC)
□ Northeast (Connecticut, Delaware, Maine, Maryland (North & Western) Massachusetts,
□ Southeast (Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi,
□ West (Alaska, Arizona, California, Colorado, Hawaii, Montana, Nevada, New Mexico)

3. What is the size of your Facility (by # of cleared employees)?

(Select only one.)

□ Less than 100
□ 100 to 500
□ 500 to 1000
□ More than 1000

4. With which of the following government contract agents does your facility have classified contracts?

   (Select all that apply.)

   □ Department of Defense (DOD)
   □ Department of Energy (DOE)
   □ Central Intelligence Agency (CIA)
   □ Nuclear Regulatory Commission (NRC)

5. Who is your Cognizant Security Agency (CSA)?

   (Select only one.)

   □ DOD
   □ DOE
   □ CIA
   □ NRC

6. From whom do you receive inspection and other NISP services?

   (Select all that apply.)

   □ DSS
   □ Other (to the extent that you can provide information)

7. Please explain if you marked "other" in the above question.

   (Provide one response only.)

   ____

   ____

Level of Knowledge

This portion of the survey will identify the security representative's level of knowledge regarding the goals and objectives of the NISP.

8. In 1994, Executive Order 12829 established the NISP, with hopes for a single, integrated industrial security program based on sound threat analysis and risk management practices. DoD became the executive agent and the processes described in the NISPOM were concurred by the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission and the Director of Central Intelligence. Are you familiar with the NISP and its creation under the Executive Order?

   (Select only one.)

   □ Yes (Skip to Q. 9)
   □ No (Skip to Q. 10)

9. If you answered yes, please take the time to elaborate and provide examples of how you became familiar with the NISP and its Executive Order?

   (Provide one response only.)

   ____

   ____

10. In January of 1995 DoD, DOE, NRC and CIA, in close coordination with Industry, created the NISPOM (National Industrial Security Program Operating Manual) which replaced the previous ISM (DoD's Industrial Security Manual for the Safeguarding of Classified Information.) Have you seen improvements in the program during the course of your involvement with classified contracts?

    (Select only one.)

    □ Yes
    □ No
    □ Don't know

11. Please explain:

    (Provide one response only.)

    ____

    ____

12. How familiar are you with the National Industrial Security Program Policy Advisory Committee (NISPPAC) and its representatives?

    (Select only one.)

    □ Highly familiar
    □ Somewhat familiar
    □ Not familiar

13. The NISPPAC is a working committee of 14 Government representatives appointed by their Agency Directors, and 8 Industry members, representing the contractor community, appointed by the Director of ISOO for a four-year term. Do you know WHO your Industry representatives are within the NISPPAC and how to contact them?

    (Select only one.)

    □ Yes
    □ No

14. Comments on the above question.

    (Provide one response only.)

    ____

    ____

Level of Confidence

This portion of the survey will identify the security representative's level of confidence regarding achievement of the NISP's goals and objectives.

15. How would you rate the quality and the timeliness of the guidance on implementing the NISPOM that you have received from your cognizant security agency(s)?

    (Select only one.)

    □ Highly Satisfactory
    □ Moderately Satisfactory
    □ Satisfactory
    □ Unsatisfactory
    □ Extremely Unsatisfactory
    □ N/A

16. Please explain.

(Provide one response only.)

17. Overall, how do you view the success of the NISP/NISPOM in achieving its overall goals and objectives?

(Select only one.)

□ Highly Satisfactory
□ Moderately Satisfactory
□ Satisfactory
□ Unsatisfactory
□ Extremely Unsatisfactory
□ N/A

18. Please explain.

(Provide one response only.)

19. Reciprocity is one of the major focuses of the NISP. Reciprocity involves the acceptance of one agency's certification by another agency without additional requirements. Is the reciprocity principal concerning facility security clearances being applied?

(Select only one.)

□ Yes
□ No
□ Don't know

20. Please explain.

(Provide one response only.)

21. Is the reciprocity principal concerning personnel security clearances being applied?

(Select only one.)

□ Yes
□ No
□ Don't Know

22. Please explain.

(Provide one response only.)

23. Have you found any of the NISP/NISPOM requirements unreasonable with respect to damage to national security that reasonably could be expected to result from unauthorized disclosure?

(Select all that apply.)

□ Yes
□ No

24. Have you found any of the NISP/NISPOM requirements unreasonable with respect to existing or anticipated threat to the disclosure of the information?

(Select only one.)

□ Yes
□ No

25. Have you found any of the NISP/NISPOM requirements unreasonable with respect to short and long-term costs?

(Select only one.)

□ Yes
□ No

26. Do you believe you have been provided adequate information with respect to the threat to classified information held by your organization?

(Select only one.)

□ Yes
□ No

27. Please explain the answers that you provided in the previous four questions (#23, 24, 25, 26).

(Provide one response only.)

28. Have you been provided clear guidance with respect to whom you should contact when in need of assistance in dealing with the NISPOM or other industrial security guidance?

(Select only one.)

□ Yes
□ No

29. Please explain.

(Provide one response only.)

Sources of Concern

This portion of the survey addresses various concerns the security representative may have regarding various functional areas within the NISP.

30. Do you have sources of concern on the granting of facility security clearances?

(Select only one.)

□ Yes (Skip to Q. 31)
□ No (Skip to Q. 32)

31. What are your sources of concern on the granting of facility security clearances?

(Provide one response only.)

32. Do you have sources of concern on the granting of personnel security clearances?

(Select only one.)

□ Yes (Skip to Q. 33)

□ No (Skip to Q. 34)

33. What are your sources of concern on the granting of personnel security clearances?

(Provide one response only.)

____

____

34. Do you have sources of concern on classification and markings?

(Select only one.)

□ Yes (Skip to Q. 35)

□ No (Skip to Q. 36)

35. What are your sources of concern on classification and markings?

(Provide one response only.)

____

____

36. Do you have sources of concern on creating, handling and storing classified information?

(Select only one.)

□ Yes (Skip to Q. 37)

□ No (Skip to Q. 38)

37. What are your sources of concern on creating, handling and storing classified information?

(Provide one response only.)

____

____

38. Do you have sources of concern on physical security issues including construction requirements, containers, and intrusion detection systems?

(Select only one.)

□ Yes (Skip to Q. 39)

□ No (Skip to Q. 40)

39. What are your sources of concern on physical security issues including construction requirements, containers, and intrusion detection systems?

(Provide one response only.)

____

____

40. Do you have sources of concern on visits, meetings, and subcontracting?

(Select only one.)

□ Yes (Skip to Q. 41)

□ No (Skip to Q. 42)

41. What are your sources of concern on visits and meetings and subcontracting?

(Provide one response only.)

____

____

42. Since its revision, does Chapter 8 of the NISPOM adequately address Automated Information Security Systems?

(Select only one.)

□ Yes

□ No

43. Please explain any problems that you have encountered with Chapter 8 since its revision.

(Provide one response only.)

____

____

44. Do you have sources of concern on International Security Requirements?

(Select only one.)

□ Yes (Skip to Q. 45)

□ No (Skip to Q. 46)

45. What is your greatest source of concern on International Security Requirements?

(Provide one response only.)

____

____

46. Do you have sources of concern on the special handling requirements for restricted data, formerly restricted data, and CNWDI data?

(Select only one.)

□ Yes (Skip to Q. 47)

□ No (Skip to Q. 50)

47. What are your sources of concern on the special handling requirements for restricted data, formerly restricted data, and CNWDI data?

(Provide one response only.)

____

____

48. Do you have sources of concern on the special handling requirements for intelligence information?

(Select only one.)

□ Yes
□ No

49. What are your sources of concern on the special handling requirements for intelligence information?

(Provide one response only.)

50. The NISPOM Supplement and Overprint were written to provide enhanced security options, which are available to augment the NISPOM 's baseline security provisions for certain sensitive and intelligence community programs. Are you familiar with these documents?

(Select only one.)

□ Yes (Skip to Q. 51)
□ No (Skip to Q. 52)

51. What are your sources of concern on the Supplements or the Overprint to the NISPOM?

(Provide one response only.)

52. The NISPOM is focused on the protection of classified information, but a renewed emphasis on "Sensitive But Unclassified" information has been experienced by many contractors. Have you received instructions from a customer on protection of "Sensitive But Unclassified" information?

(Select only one.)

□ Yes (Skip to Q. 53)
□ No (Skip to Q. 54)

53. Please explain the situation where you did receive instruction and detail the instructions that were given to you.

(Provide one response only.)

54. Do you believe that the NISPOM adequately addresses the handling of "Sensitive But Unclassified" information?

(Select only one.)

□ Yes
□ No
□ Don't Know

55. Have you ever been instructed or encouraged to utilize physical protection and/or access and dissemination controls for the protection of "Sensitive But Unclassified" information?

(Select only one.)

□ Yes
□ No

Success of the NISP

This portion of the survey asks your opinion on the success of the NISP.

56. Are there specific areas in which implementation of the NISP has achieved the objectives of the Executive Order for a single, integrated, security program based on sound threat analysis and risk management practices?

(Select only one.)

□ Yes
□ No

57. Please explain and elaborate on areas that you feel the NISP has achieved, or failed to achieve, its objectives.

(Provide one response only.)

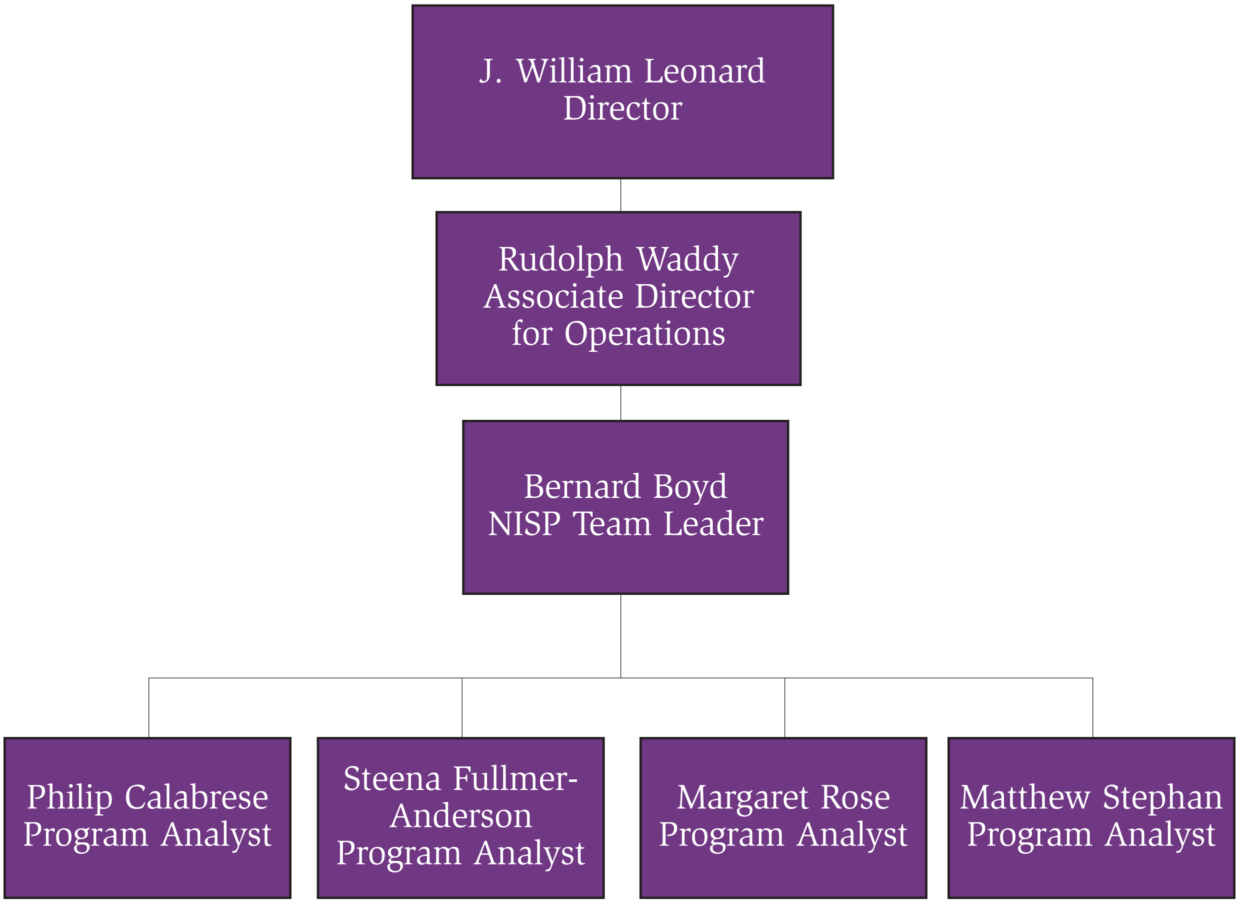
58. Please elaborate and provide examples of ways to improve the NISP to fit the needs of your organization.

(Provide one response only.)

APPENDIX B
ISOO'S ON-SITE INTERVIEW QUESTIONS

1. How long have you been involved with classified contracts? During the course of your involvement with classified contracts under the NISP, have you seen or experienced improvements in the manner or way in which clearances are handled or information is safeguarded?
2. Do you know who your industry representatives are within the NISPPAC and how to contact them?
3. Reciprocity is one of the major focuses of the NISP. Reciprocity involves the acceptance of one Agency's certification by another Agency without additional requirements. Is the reciprocity principle concerning facility security clearances being applied?
4. Do you have sources of concern on the granting of personnel security clearances? Do you feel that the reciprocity principle concerning personnel security clearances is being applied? Specifically, in the personnel security area, do you find reciprocity agreements eroding, causing an impact on time, money or personnel resources?
5. Have you found any of the NISP/NISPOM requirements unreasonable with respect to short-term and long-term cost?
6. Do you have sources of concern on classification markings? If so, what are they?
7. Since it's revision, does Chapter 8 of the NISPOM adequately address Automated Information Security Systems? From your perspective, are there any specific problems that still linger?
8. Do you have any classified contracts with foreign interests? Do you have sources of concern on international security requirements, such as receiving proper disclosure guidance from your CSA?
9. The NISPOM Supplement and Overprint were written to provide enhanced security options, which are available to augment the NISPOM's baseline security provisions for certain sensitive and intelligence community programs. Are you familiar with these documents? Do you have a source of concern on the Supplements or the Overprint to the NISPOM? If so, what are they?
10. The NISPOM is focused on the protection of classified information, but a renewed emphasis on "Sensitive but Unclassified (SBU)" information has been experienced by many contractors. Have you received instructions from a customer on protection of "SBU" information? Please explain the situation where you did receive instruction and the level of detail given to you.
11. Have you been successful in receiving adequate and timely threat information from your CSA or another government source?
12. Do you believe there has been an adequate review of your programs to assess security vulnerabilities that could be exploited? In the wake of 9/11, has your company had to reassess or bolster its security operations internally? If so, how?
13. Based on your experience, please elaborate and provide examples of ways to improve the NISP to fit the needs of your organization.

APPENDIX C
ISOO'S NISP TEAM



J. William Leonard
Director

Rudolph Waddy
Associate Director
for Operations

Bernard Boyd
NISP Team Leader

Philip Calabrese
Program Analyst

Steena Fullmer-Anderson
Program Analyst

Margaret Rose
Program Analyst

Matthew Stephan
Program Analyst

* This chart represents the composition of the NISP team for the 2002 survey.

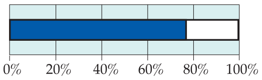
APPENDIX D
ACRONYMS AND ABBREVIATIONS

AIS	Automated Information System
AISSP	Automated Information System Security Plan
ANSIR	Awareness of National Security Issues and Response
CIA	Central Intelligence Agency
CFISAC	Central Florida Industrial Security Awareness Council
CNWDI	Critical Nuclear Weapons Design Information
C	Confidential
CSA	Cognizant Security Agency
CVA	Central Verification Activity
DD 254	Department of Defense 254
DHS	Department of Homeland Security
DISCO	Defense Industrial Security Clearance Office
DSS	Defense Security Service
DOD	Department of Defense
DOHA	Defense Office of Hearings and Appeals
DOE	Department of Energy
E.O.	Executive Order
EPSQ	Electronic Personnel Security Questionnaire
FBI	Federal Bureau of Investigation
FAISSR	Florida Association of Information Systems Security Representatives
FAST	Feedback and Automated Systems Security Plan Template
FOUO	For Official Use Only
FRD	Formerly Restricted Data
FSO	Facility Security Officer
ICSE	Interagency Committee on Security Equipment
ISL	Industrial Security Letter
ISP	Information Security Plan
ISM	Industrial Security Manual
ISOO	Information Security Oversight Office
ISSR	Information System Security Representative
ISTAC	Information Systems Technology Advisory Committee
LOC	Letter of Notification of Personnel Clearance
LOU	Limited Official Use
NSP	Network Security Plan
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISPPAC	National Industrial Security Program Policy Advisory Committee
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSP	Network Security Plan
OPM	Office of Personnel Management
OPSEC	Operations Security
OUO	Official Use Only
PCL	Personnel (Security) Clearance
S	Secret
SAP	Special Access Program
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmentalized Information
SSP	System Security Plan
S/TAR	Secure Tape Archive
TS	Top Secret

APPENDIX E
CHARTS AND GRAPHS

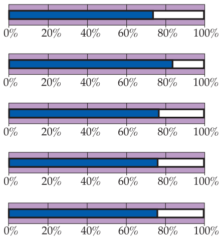
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 10 (binary): I have seen improvements in the program during the course of my involvement with classified contracts.	244	185	76%



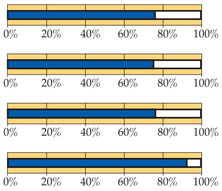
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	85	61	72%
Southeast region	54	45	83%
Northeast region	34	26	76%
Central region	20	15	75%
Capital region	51	38	75%
TOTAL:	244	185	76%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	133	98	74%
100 to 500 cleared employees	52	38	73%
500 to 1000 cleared employees	24	18	75%
More than 1000 cleared employees	35	31	89%
TOTAL:	244	185	76%



Statistical interpretation of the data:

Differences in the proportion of positive responses among the five regions were not statistically significant.

Differences in the responses among the four company sizes were not statistically significant. Though the numbers of facilities that responded in the pejorative to this question are low, that does not necessarily mean that there are problems. Additionally, a large number of respondents have only been in their positions for 1 or 2 years and may not have the historical perspective to see improvements.

Relevant comments from the community:

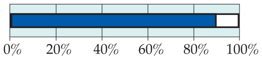
"Primary improvements appeared with the implementation of the NISPOM, which more concisely delineated procedures for submission of various reports. In addition, the implementation of the Electronic Personnel Security Questionnaire (EPSQ) program and subsequent establishment of the Defense Security Service (DSS) web site greatly improved accessibility to data regarding the National Industrial Security Program (NISP) and provided access to on-line identification of approved personnel (security) clearances (PCLs) without having to wait for mail confirmation."

"The improvements are mostly more cost efficient for both the contractor and the government as it pertains to more relaxed user friendly directives within the NISPOM. However, because the NISPOM places more of an emphasis on contractor responsibility in applying the NISPOM to daily practical Industrial Security issues, sometimes the less specific and detailed paragraphs within the NISPOM need clarification from the ISSR. This presents a problem of interpretation in a lot of cases. I have noticed at times that some DSS Reps differ in their interpretations of the not so detailed NISPOM. Many times though this has been resolved by questions and answers provided to the contractors in ISL on controversial issues."

"Cleared employees with current investigations with one agency can now access another agencies information based on need-to-know. Visit procedures are stream lined. Accreditation of an area previously approved by one CSA can now be accomplished by another CSA quicker."

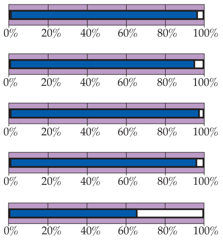
Overall Response

Question	Highly satisfactory	Satisfactory	Unsatisfactory	Extremely unsatisfactory	Moderately satisfactory *	# of responses	# of yes responses	% of yes responses
Question 17 (multiple choice): Overall, how do you view the success of the NISP/NISPOM in achieving its overall goals and objectives?	103	122	24	2	124	251	225	90%



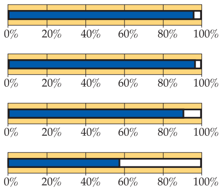
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	85	82	96%
Southeast region	47	44	94%
Northeast region	40	39	98%
Central region	28	27	96%
Capital region	51	33	65%
TOTAL:	251	225	90%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	168	159	95%
100 to 500 cleared employees	33	32	97%
500 to 1000 cleared employees	18	16	89%
More than 1000 cleared employees	32	18	56%
TOTAL:	251	225	90%



Statistical interpretation of the data:

*The "Moderately Satisfactory" responses were excluded from the analysis due to their non-contributive nature.

Differences in the responses among the five regions were found to be statistically significant ($p < 0.05$). No obvious pattern was found for these differences though it should be noted that respondents from the Capital Region did show a lower percentage of positive responses to this question when compared to responses from the other four regions of the country.

Differences in the responses among the four company sizes were found to be statistically significant ($p < 0.05$). No obvious pattern was found for these differences, though it should be noted that facilities with more than 1000 cleared employees did show a lower percentage of positive responses to this question when compared to responses from the other 3 facility sizes.

Relevant comments from the community:

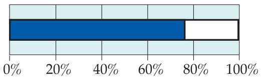
"My company followed NISPOM guidance to prepare the documents required for accreditation of our facilities and information systems. Our DSS representatives directed us to disregard the NISPOM and follow document templates they provided instead. Thus, the goal of using the NISPOM as a basis for standardization is not being met."

"The NISP has given the contractors the opportunity to be more of a partner with DSS rather than being an enemy. It has given us the opportunity to applying risk management in the safeguard of classified materials. This has allowed us to meld security into our business strategies and into our programs from inception thereby us to reduce the cost of security processes, protect classified materials from cradle to grave and to keep up with production schedules without sacrificing our nations secrets."

"It has not eliminated multiple-agency inspections; has not resulted in eliminated double-reporting (apparently other agencies will not accept a verification of facility clearance by DSS (CVA); classified visit requests are not standardized; agencies still require a new Standard Form 86 rather than accepting DISCO personnel security clearances; non-disclosure agreements still not universally accepted."

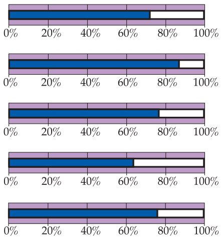
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 19 (binary): The reciprocity principle concerning facility security clearances is being applied.	217	161	74%



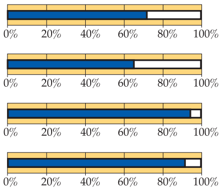
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	78	54	69%
Southeast region	42	37	88%
Northeast region	30	22	73%
Central region	21	13	62%
Capital region	46	35	76%
TOTAL:	217	161	74%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	124	86	69%
100 to 500 cleared employees	37	24	65%
500 to 1000 cleared employees	21	20	95%
More than 1000 cleared employees	35	31	89%
TOTAL:	217	161	74%



Statistical interpretation of the data:

Differences in the responses among the five regions were not statistically significant.

Differences in the responses among the four company sizes were found to be statistically significant ($p < 0.05$), however no obvious pattern was found for these differences.

This question does not address whether a responding facility has ever gone through this process and positive responses may be from facilities that have never gone through the process, or who have limited experience with it, and therefore have never had a problem. Additionally, it appears from the one-on-one interviews that most people misunderstand this question when first presented with it.

Relevant comments from the community:

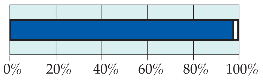
"DSS is apparently incapable of processing reciprocity in situations where an existing facility clearance exists under a classified relationship between the contractor and the Government. We found ourselves in this situation, and our existing sponsor repeatedly communicated data about our existing facility clearance to DSS. However, DSS repeatedly failed to get that information into the hands of our assigned DSS representatives. We were thus forced to start over—and proceed with no reciprocity."

"I am a DoD cleared facility with a large DOE contract. Some examples of reciprocity are the DOE accepts DoD facility clearance and personnel clearances, closed area designations and DoD certification of classified processing systems."

"I've never had to do one on the DoD side, but I do know that reciprocity on the SCI side of the house works well and is greatly appreciated by industry. It cuts out security costs, time and effort to start up and get running."

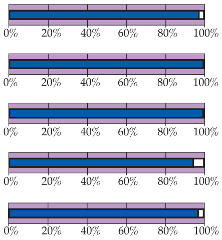
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 28 (binary): I have been provided clear guidance with respect to whom I should contact when in need of assistance in dealing with the NISPOM or other industrial security guidance.	393	386	98%



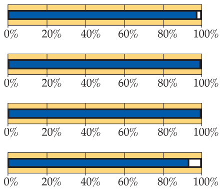
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	140	137	98%
Southeast region	77	77	100%
Northeast region	69	69	100%
Central region	44	42	95%
Capital region	63	61	97%
TOTAL:	393	386	98%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	260	256	98%
100 to 500 cleared employees	62	62	100%
500 to 1000 cleared employees	28	28	100%
More than 1000 cleared employees	43	40	93%
TOTAL:	393	386	98%



Statistical interpretation of the data:

Differences in the proportion of positive responses among the five regions were not statistically significant.

Differences in the responses among the four company sizes were not statistically significant.

Relevant comments from the community:

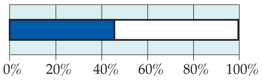
"Absolutely. Our DSS Rep. is excellent. We know his district supervisor. They have been more than helpful over the years."

"The local DSS office does an OUTSTANDING job of supporting our facility. Our DSS Rep. goes well above the call of duty in supporting us and our other Customers. The local DSS-Field Chief is extremely responsive and willing to "think out of the box" to help us meet our contract goals and maintain National Security objectives."

"I'm largely a self-taught FSO. If I can't find the answer independently I use a "networking" approach to other FSOs, call the DSS Customer Service Office or ask my DSS Rep."

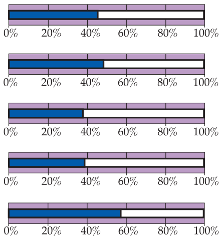
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 32 (binary): I have sources of concern on the granting of personnel security clearances.	393	179	46%



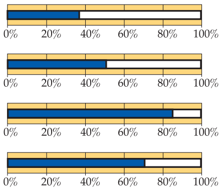
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	141	64	45%
Southeast region	77	36	47%
Northeast region	69	26	38%
Central region	44	17	39%
Capital region	63	36	57%
TOTAL:	394	179	45%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	260	95	37%
100 to 500 cleared employees	62	31	50%
500 to 1000 cleared employees	28	24	86%
More than 1000 cleared employees	43	29	67%
TOTAL:	393	179	46%



Statistical interpretation of the data:

Differences in the proportion of positive responses among the five regions were not statistically significant.

Differences in the responses among the four company sizes were found to be statistically significant ($p < 0.05$). The cause of these differences could be attributed to the fact that a facility with a greater number of cleared employees would have to go through the process of clearing employees more often than a smaller facility and therefore would have more opportunities for problems in the system.

Relevant comments from the community:

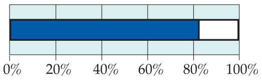
"The backlog is outrageous and unacceptable. Many contractors have employees who have been "in process" for more than two years. Processing conversions, reinstatements, and the like are taking 30-45 days, or more. Interim clearances are being granted to individuals with "affirmatives" in the privacy section; final clearances are being granted when the investigation hasn't been completed and discovered when the investigator arrives at the facility."

"I have recently gone through an exercise with my local Field Office Chief for Investigations concerning over 100 "interim" clearances that we have, some dating back to 1998. He spent a considerable amount of time tracking down information on these cases. In the end we determined that the DISCO has no record on a couple of the personnel that we have been awaiting final clearances on, over a dozen cases are considered adjudicated and closed by the DISCO, however no LOC was ever issued to us; a couple of the cases are "thought" to be with contractors; and over 40 of the cases are sitting at DOHA for adjudication."

"Some of the clearance requests have taken very long to process. We have seen a significant improvement though in the past year with interim clearances being issued more expeditiously. Another concern is the new LOC electronic system. We have noticed from "Meade Listings" that clearances for individuals have been issued but we have never seen a LOC for the individual. Because of this problem, we would like to see quarterly validation listings effected."

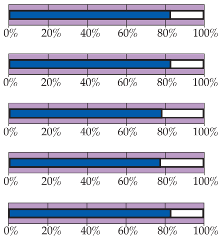
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 42 (binary): Since its revision, Chapter 8 of the NISPOM adequately address Automated Information Security Systems.	393	320	81%



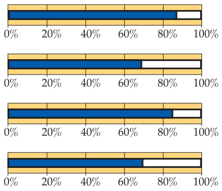
Breakdown by Region

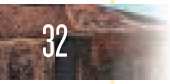
	# of responses	# of yes responses	% of yes responses
Western region	140	115	82%
Southeast region	77	64	83%
Northeast region	69	54	78%
Central region	44	34	77%
Capital region	63	53	84%
TOTAL:	393	320	81%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	260	225	87%
100 to 500 cleared employees	62	42	68%
500 to 1000 cleared employees	28	23	82%
More than 1000 cleared employees	43	29	67%
TOTAL:	393	319	81%





Statistical interpretation of the data:

Differences in the responses among the five regions were not statistically significant.

Differences in the responses among the four company sizes were found to be statistically significant ($p < 0.05$) however, no obvious pattern was found for these differences.

Comments in the essay portion of this question, along with onsite interview responses, show a high level of concern with the implementation of Chapter 8. This question in its present state does not address these concerns.

Relevant comments from the community:

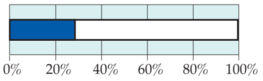
"Overall, it's much better now than before. However, the DSS ISSRs around the country need to interpret and apply these regulations more consistently. Also, DSS has not kept up with the pace of change in technology when it comes to Trusted Download procedures. In my opinion, the currently approved procedures posted on their website are very inadequate for current Microsoft products like Word and PowerPoint and they represent a risk to national security. Also, their trusted software utilities (such as ISTAC or S/TAR) are out of date and incompatible with current hardware."

"Some ISSRs do not like "boiler plates" available (FAISSR) and will NOT approve procedures based on those. There needs to be some consistency across DSS. If it is a good plan (won the Information Security Award at NCMS), hailed by Gen. Iverson, then IS reps should be happy to approve plans based on the FAISSR boilerplate... as long as necessary adjustments for each facility have been made. That isn't happening..."

"Yes, I was in charge of writing up our AIS system and Ch. 8 of the NISPOM was VERY helpful in doing that. I went on the DSS website and they had an outline of what changed versus what it used to be and that was so very helpful because I had everything right in front of me."

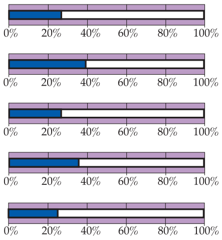
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 52 (binary): I have received instructions from a customer on protection of "Sensitive But Unclassified" information.	393	114	29%



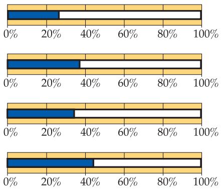
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	140	36	26%
Southeast region	77	30	39%
Northeast region	69	18	26%
Central region	44	15	34%
Capital region	63	15	24%
TOTAL:	393	114	29%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	260	62	24%
100 to 500 cleared employees	62	23	37%
500 to 1000 cleared employees	28	9	32%
More than 1000 cleared employees	43	20	47%
TOTAL:	393	114	29%



Statistical interpretation of the data:

Differences in the responses among the five regions were not statistically significant.

Differences in the responses among the four company sizes were found to be statistically significant ($p < 0.05$), however no obvious pattern was found for these differences.

Comments from the community:

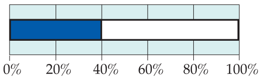
"DOE has provided extensive direction in this area. In some regards perhaps too much. I say this because it seems we have a new category of unclassified but sensitive information to deal with every few months. In a couple of instances the instructions were changed once it was discovered the full impact of implementation. We do try and look at what we are doing to protect our operations and OPSEC is a big part of our daily lives."

"The word "Sensitive" is being misapplied every day in DoD. Congress added the language into a DOE bill that stated a contractor would be fined for a security incident and it included the term "sensitive" information. DOE is still trying to figure out what "sensitive" information is. In addition, the word "sensitive" is used in the military to sometimes denote classified information. We all know there are still three levels of classification TS, S, and C. So I have briefed my people if they hear the term to call me so that I can make a determination of what is really meant by the use of the word. It has added to the confusion."

"The instructions are always VERBAL! I have documents that are marked Unclassified—Handle via SAP Channels Only. It is difficult to explain or understand the requirement to protect unclassified information. This is one of those requirements that makes the security profession look silly."

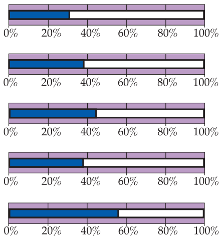
Overall Response

	# of responses	# of yes responses	% of yes responses
Question 54 (binary): The NISPOM adequately addresses the handling of "Sensitive, But Unclassified" information.	224	90	40%



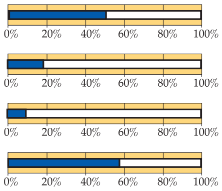
Breakdown by Region

	# of responses	# of yes responses	% of yes responses
Western region	71	21	30%
Southeast region	49	19	39%
Northeast region	30	14	47%
Central region	24	9	38%
Capital region	50	27	54%
TOTAL:	224	90	40%



Breakdown by No. of Cleared Employees

	# of responses	# of yes responses	% of yes responses
Less than 100 cleared employees	124	60	48%
100 to 500 cleared employees	40	7	18%
500 to 1000 cleared employees	24	2	8%
More than 1000 cleared employees	36	21	58%
TOTAL:	224	90	40%



Statistical interpretation of the data:

Differences in the responses among the five regions were found to be statistically significant ($p < 0.05$), however no obvious pattern was found for these differences.

Differences in the responses among the four company sizes were found to be statistically significant ($p < 0.05$), however no obvious pattern was found for these differences.

Comments from the community:

"At this time I do not believe the DSS should be concerned with SBU but rather DSS should focus on what they do well and that is the protection of classified information. I believe that contractors who safeguard their proprietary information should apply their same procedures for protecting SBU information."

"I don't know because frequently I don't know what the government procurement office(s) want protected. If it is MARKED with a CLASSIFICATION, we know what to protect and how to protect but UNCLASSIFIED is more difficult."

"Industry has had a concern for handling sensitive unclassified information for over 10 years if not longer. I don't know if it is appropriate to place this caveat within NISP. Something has to be formalized whether it is an E.O. or ISL. The DD 254 covers FOUO but the issue is much bigger than FOUO. Industry recognizes the immensity of this effort and is struggling with defining SBU. Not every contract has a DD 254 so we need a more comprehensive vehicle."

"The NISPOM appears to cover every conceivable situation. It clearly spells out responsibilities and practices. Common sense is required by the contractor, but familiarity with the NISPOM, and the occasional question to the DSS Rep, results in confidence that sensitive information is being well protected."

Comments from ISOO's Town Hall Meeting at the 2003 National Classification Management Society Conference, Salt Lake City, Utah

"...to get immediate answers from "upper level" people is a great opportunity."

"They (DoD and DSS) were frank and honest. This is the type of interaction that is most helpful."

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) CONTACT INFORMATION

THE INFORMATION SECURITY OVERSIGHT OFFICE

Director | National Archives and Records Administration Building
700 Pennsylvania Avenue, N.W., Room 500 | Washington, D.C. 20408
(202) 219-5250 | www.archives.gov/isoo | Email: nisp@nara.gov

CENTRAL INTELLIGENCE AGENCY (CIA)

Director of Security
Washington, D.C. 20505 | (703) 482-9006

DEPARTMENT OF ENERGY (DOE)

Director, Office of Security
1000 Independence Avenue SW | Mail Stop: SO-1
Washington, D.C. 20585 | (202) 586-3345
Email: energy.nisp@hq.doe.gov

NUCLEAR REGULATORY COMMISSION (NRC)

Director of Facilities and Security
Mail Stop-T7D57 | Washington, D.C. 20555 | (301) 415-8080
Email: tom2@nrc.gov

THE OFFICE OF THE SECRETARY OF DEFENSE

Director of Industrial Security | OUSD (I)
Room 3E194, 5000 Pentagon | Washington, D.C. 20301
(703) 695-9468

DEFENSE SECURITY SERVICE

Deputy Director for Industrial Security Program
1340 Braddock Place | Alexandria, VA 22314-1651 | (888) 282-7682
Email: occ_cust_serv@mail.dss.mil

INDUSTRY

For information on the industry representatives, please contact ISOO at the e-mail address or telephone number mentioned above.

INFORMATION SECURITY OVERSIGHT OFFICE