Report on Cost Estimates for Security Classification Activities

Background and Methodology

As part of its responsibilities to oversee agency actions to ensure compliance with Executive Order (E.O.) 12958, as amended, "Classified National Security Information," and E.O. 12829, as amended, "National Industrial Security Program," (NISP), ISOO annually reports to the President on the estimated costs associated with the implementation of these Orders. This marks the 12th year of reporting these costs for security classification activities to include safeguarding requirements.

In the past, the costs for the implementation of the programs to classify, safeguard, and declassify national security information were deemed non-quantifiable, intertwined with other overhead expenses. While portions of the program's costs remain ambiguous, ISOO continues to collect cost estimate data and to monitor the methodology used for its collection. Requiring agencies to provide exact responses to the cost collection efforts would be cost prohibitive. Consequently, ISOO relies on the agencies to estimate the costs of the security classification system. The collection methodology has remained stable over the past 12 years, providing a good indication of the trends in total cost. Nonetheless, it is important to note that absent any security classification activity, many of the expenditures reported herein would continue to be made in order to address other, overlapping security requirements.

The data for Government presented in this report were collected by categories based on common definitions developed by an Executive branch working group. The categories are defined as follows:

Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Information Security: Includes three subcategories:

- **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting classified information from unauthorized disclosure, the protection of which is authorized by executive order or statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, or destroy classified information.
- **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, and mandatory declassification review programs authorized by Executive order, as well as declassification activities required by statute.
- **Information Systems Security for Classified Information:** An information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Security of these

systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. It can include, but is not limited to, the provision of all security features needed to provide an accredited system of protection for computer hardware and software, and classified information, material, or processes in automated systems.

Professional Education, Training and Awareness: The establishment, maintenance, direction, support, and assessment of a security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

Security Management and Planning: Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Unique Items: Those department-or agency-specific activities that are not reported in any of the primary categories but are nonetheless significant and need to be included.

Survey Results and Interpretation

The total security classification cost estimate within Government for FY 2006 is $8.2 billion. This figure represents estimates provided by 41 executive branch agencies, including the Department of Defense. It does not include, however, the cost estimates of the Central Intelligence Agency (CIA), the National Geospatial Intelligence Agency (NGA), the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA), which those agencies have classified in accordance with Intelligence Community classification guidance.

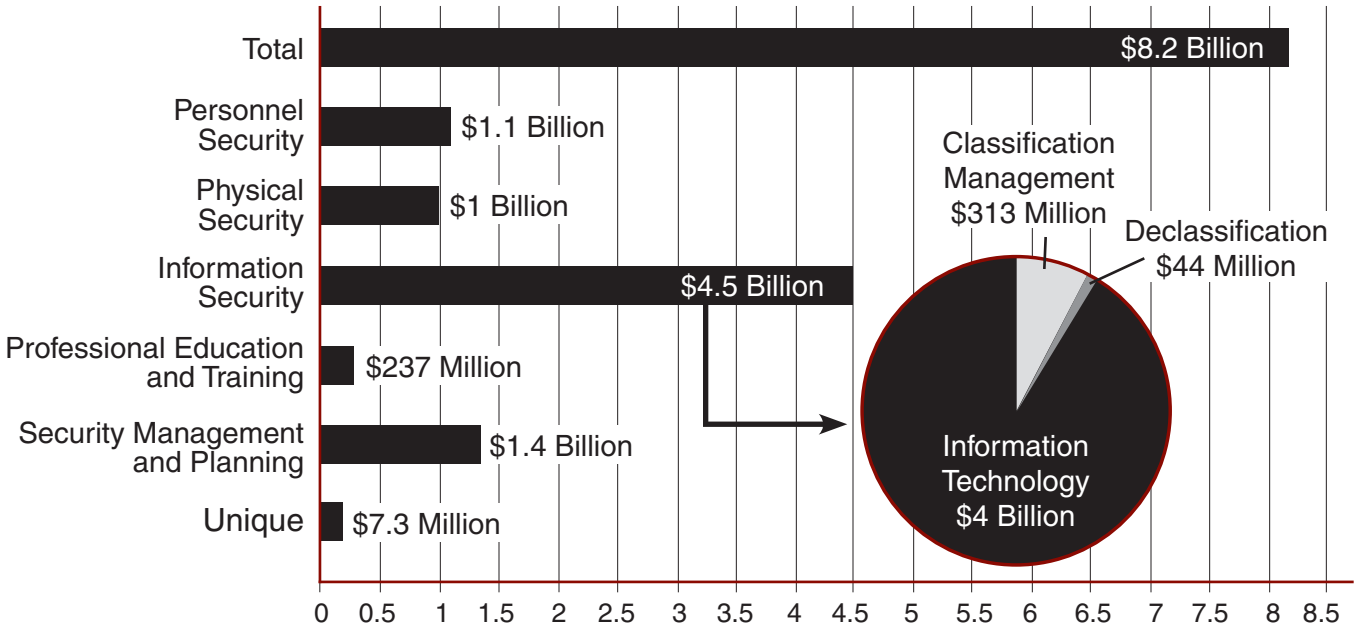
A joint Department of Defense and industry group developed a cost collection methodology for those costs associated with the use and protection of classified information within industry. Because industry accounts for its costs differently than Government, cost estimate data are not provided by category. Rather, a sampling method was applied that included volunteer companies from four different categories of contractor facilities. The category of facility is based on the complexity of security requirements that a particular company must meet in order to hold and perform under a classified contract with a Government agency.

The 2006 cost estimate totals for industry pertain to the twelve-month accounting period for the most recently completed fiscal year of each company that was part of the industry sample. For most of the companies included in the sample, December 31, 2006, was the end of their fiscal year. The estimate of total security classification costs for 2006 within industry was $1.2 billion.

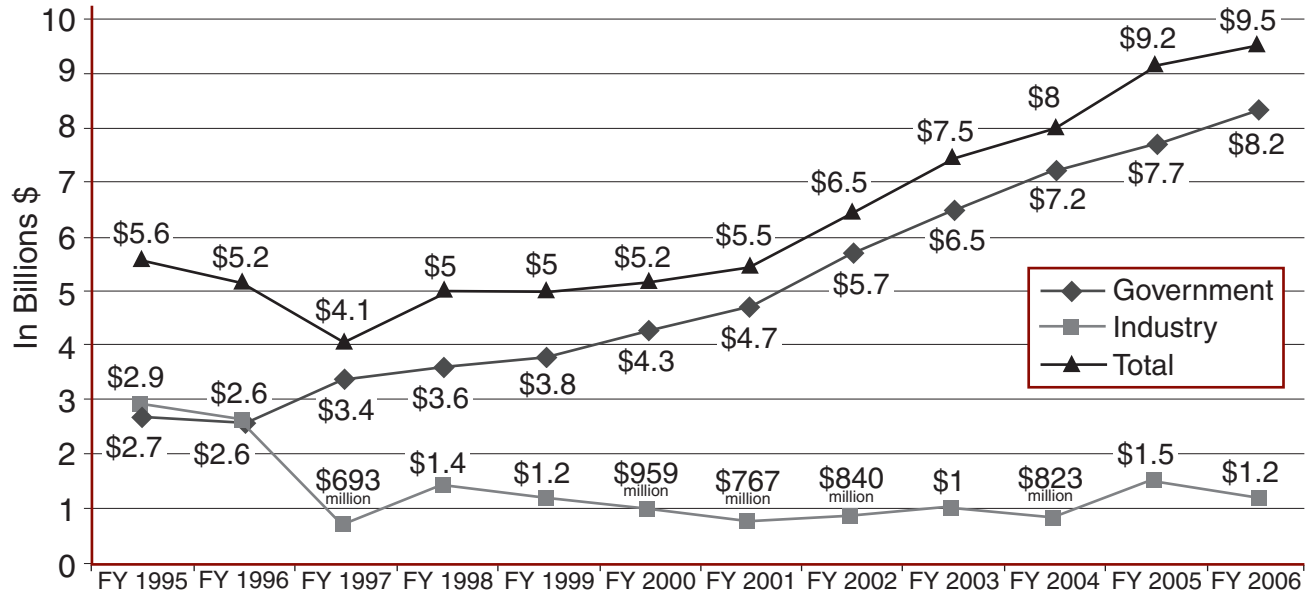
As stated previously, the Government cost estimate for FY 2006 is $8.2 billion, which is a $573 million, or 7.5 percent increase, above the cost estimates reported for FY 2005. The industry estimate is down by $263 million. This makes the total 2006 cost estimate for Government and industry $9.5 billion, which is $278 million more than the total FY 2005 cost estimate for Government and industry. This is a 3 percent increase in the Government plus industry figures, which is roughly equal to the average rate of inflation for that same time period.

The largest increase came from the Information Systems Security category, which experienced a $381 million, or 10.5 percent, increase. Many

Government Security Classification Costs Estimate Fiscal Year 2006



Graph comparing total costs for government and industry for FY 1995-2006



agencies that have never before had secure information networks are acquiring access to these networks in the interest of information sharing. In this same vein, several agencies report that they are still developing Sensitive Compartmented Information Facilities (SCIFs), emergency operational control centers, and Continuity of Operations (COOP) sites. Nevertheless, it appears that this sort of activity is leveling off since Physical Security costs only increased by 1.7 percent.

Some agencies are still reporting large increases in Personnel Security costs due to the requirement to implement the newly established standards for Personal Identity Verification (PIV) throughout the Executive branch by October 2006. Even so, the total reported expenditures in this category actually declined by 3.5 percent which suggests that the bow wave in requirements for personnel security investigations may have passed.

The reported amount spent on declassification declined by 22.6 percent even though the number of pages reviewed and the number of pages declassified actually increased. We believe this was possible because the intelligence agencies account for a very large segment of the declassification numbers and their financial data is not included in this report.

Professional Education, Training, and Awareness continued to rise in FY 2006, this time by 8.3 percent. Many agencies continue to develop state-of-the-art information security training products that are capable of reaching wide audiences, and they are also using private industry experts to assist with training management.

There was a large spike in the figures reported for the Miscellaneous (OPSEC & TSCM) category, which is due to DoD discovering TSCM resources that had previously been reported under the Information Systems Security category.

Conclusion

As noted last year, the rate of increase in the security cost estimates reported by the Executive branch agencies has apparently leveled off after the surge in security requirements and programs generated by the homeland defense concerns in the post-2001 environment. We also continue to see positive movement in categories such as training, and oversight and planning, which are important areas that ISOO frequently finds lacking during its security program reviews.