



## **REPORT ON COST ESTIMATES FOR SECURITY CLASSIFICATION ACTIVITIES FOR 2005**

### **BACKGROUND AND METHODOLOGY**

As part of its responsibilities to oversee agency actions to ensure compliance with Executive Order 12958, as amended, "Classified National Security Information," and Executive Order 12829, as amended, "National Industrial Security Program," (NISP), the Information Security Oversight Office (ISOO) annually reports to the President on the estimated costs associated with the implementation of these Orders. This marks the 11th 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 11 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 presented in this report for Government were collected by categories based on common definitions developed by an executive branch working group. The categories are defined below.

**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 or mandatory review programs authorized by Executive order or 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.

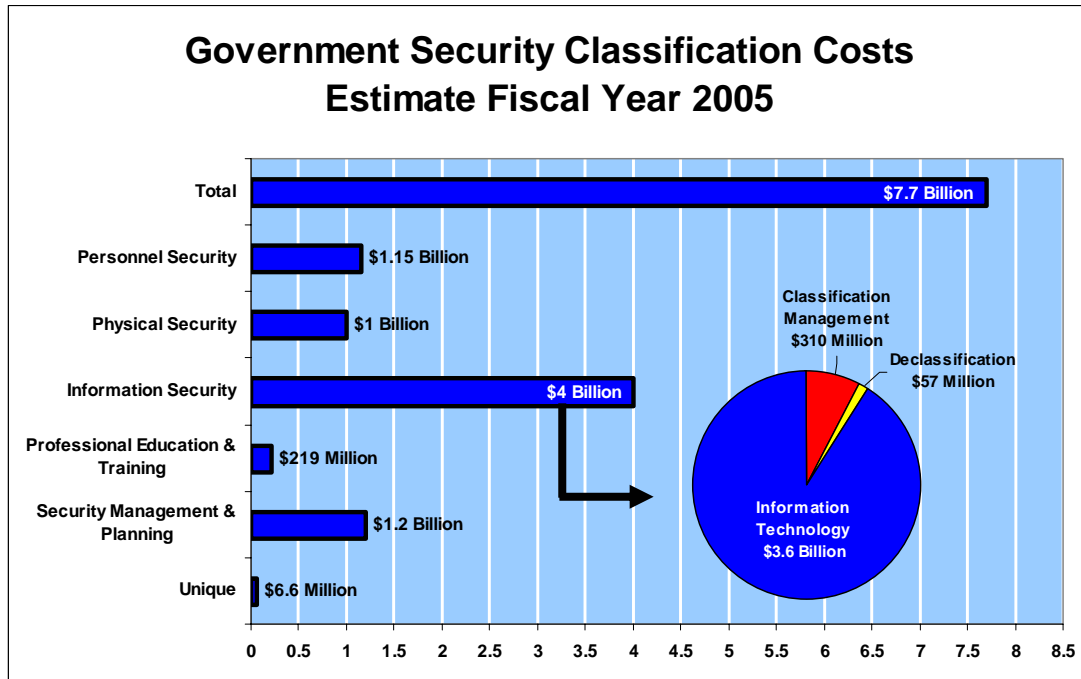
**Security Management and Planning:** Development and implementation of plans, procedures and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities and respond to management requests related to classified information.

**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 estimates within Government for FY 2005 is \$7.7 billion. This figure represents estimates provided by 41 executive branch agencies, including the

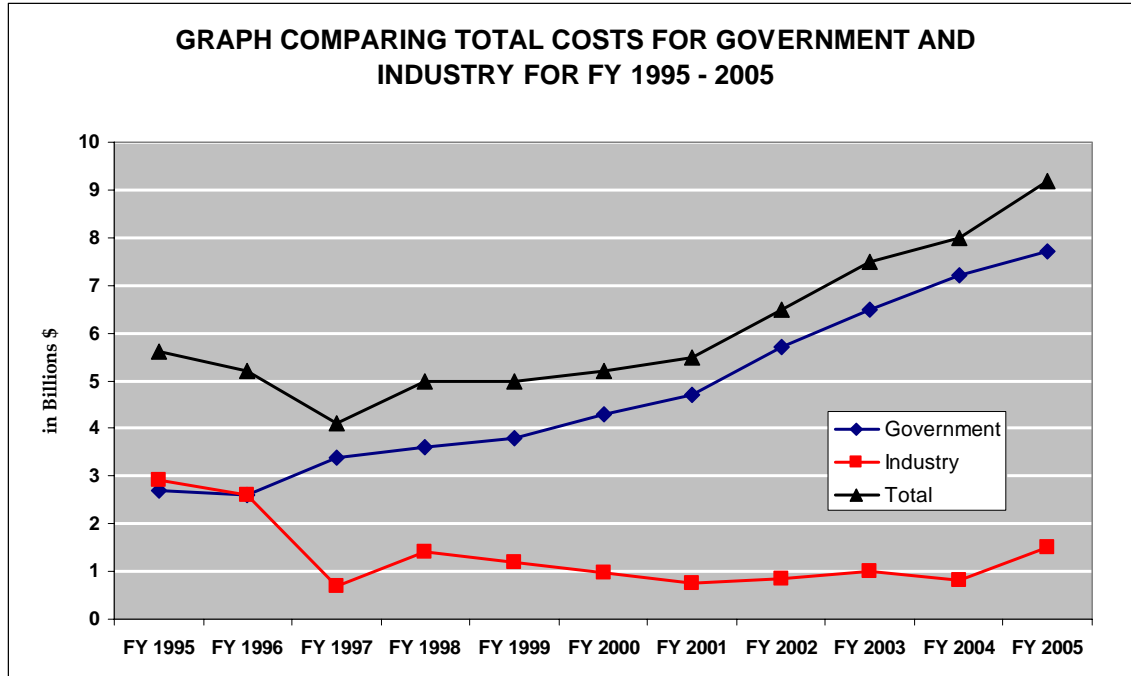
Department of Defense. It does not include, however, the cost estimates of the Central Intelligence Agency (CIA), which that agency has classified.



A joint Department of Defense (DoD) 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 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 2005 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, 2005, was the end of their fiscal year. The estimate of total security classification costs for 2005 within industry was \$1.5 billion.

The Government cost estimate for FY 2005 is \$7.7 billion, which is a \$420 million, or 5.8 percent increase above the cost estimates reported for FY 2004. The industry estimate is up by \$696 million. This makes the total 2005 cost estimate for Government and industry \$9.2 billion, which is \$1.2 billion more than the total FY 2004 cost estimate for Government and industry.



The main driver of the FY 2005 increase was Physical Security category which was up 348 million or 50 percent. Similar to the reason for last year's increase, the fortified homeland defense posture being adopted by many agencies in response to the September 11, 2001 terrorist attacks generated most of the costs associated with this category. In the FY 2004 cost estimate report, we noted that many agencies were procuring secure facilities and communications systems that they never had in the past. A number of agencies were in the process of building Sensitive Compartmented Information Facilities (SCIFs) and emergency operational control centers. In the FY 2005 cost analysis narratives agencies continue to report new requirements for the construction and equipping of SCIFs. They also report requirements for additional security containers and for systems to protect national security information. Further, a significant number of agencies are upgrading protection for field facilities to include intrusion detection and access control systems, secure communication systems, and increases in number and salary requirements for an enlarged, better equipped, and better trained guard force. Along with this many agencies are still dealing with the requirement to develop Continuity of Operations (COOP) sites, which in turn generates the need for more secure facilities and communications.

After Physical security the next largest increase came from the Personnel Security category which was up by 207 million or 22 percent. A significant number of agencies report a rise in personnel security costs due to substantially increased investigation and reinvestigation requirements. Additionally, the requirement to implement the newly established standards for Personal Identity Verification (PIV) throughout the executive branch by October 2006 is still in progress and has necessitated increased expenditures.

One noteworthy development was that Professional Education, Training, and Awareness increased by \$41 million or 23 percent. Similar to last year, agencies reported significant

emphasis on the development of new information security training products that are capable of reaching wider audiences. Several reported the utilization of private industry experts to assist with design, development, implementation, and management of training programs. These programs include both initial and refresher security training along with physical security, courier, program management, professional development, industrial security, and communications security courses.

Another noteworthy development was that cost estimates for Declassification programs increased by \$57 million or 18 percent. A few agencies have discovered that previous planning has not adequately prepared them to meet current and future declassification mandates, and are now allocating increased funds and dedicating additional manpower to this vital program element.

The Security Management, Oversight, and Planning category experienced an increase of \$67 million or 5.9 percent.. There are various reasons for the increase, such as relocation and changes in mission, acquiring additional personnel to conduct reviews and monitor policy compliance, automation of security processes, notably forms, policies, issues, and publications. There is a continued emphasis on planning for SCIF and collateral facility construction, augmenting information security training programs, security manpower, and the development of databases to track program elements, such as training, facility and system accreditations, SCI clearances, and security equipment.

## **CONCLUSION**

The rate of increase in the security cost estimates reported by the Executive branch agencies continues to slow, which suggests a stabilization of the surge in security requirements and programs generated by the homeland defense concerns in the post-2001 environment. The DoD, as Executive Agent for the National Industrial Security Program, was unable to provide a specific explanation for the large increase in the industry cost estimate, due to the methodology used to collect these data which does not provide for the inclusion of textual comments or explanations.