REPORT ON COST ESTIMATES FOR SECURITY CLASSIFICATION ACTIVITIES FOR 2004

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," 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 tenth 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 many 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 ten 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.

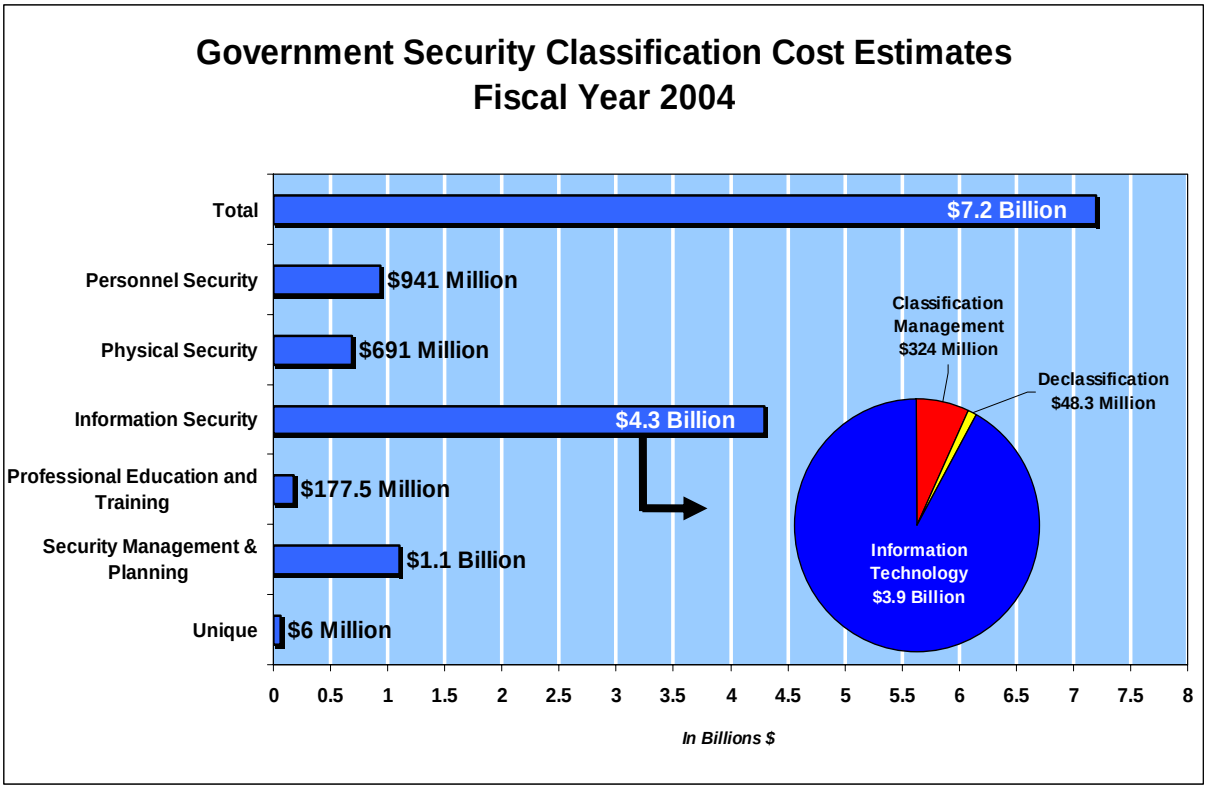
Professional Education, Training and Awareness: The establishment, maintenance, direction, support and assessment of a security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel 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

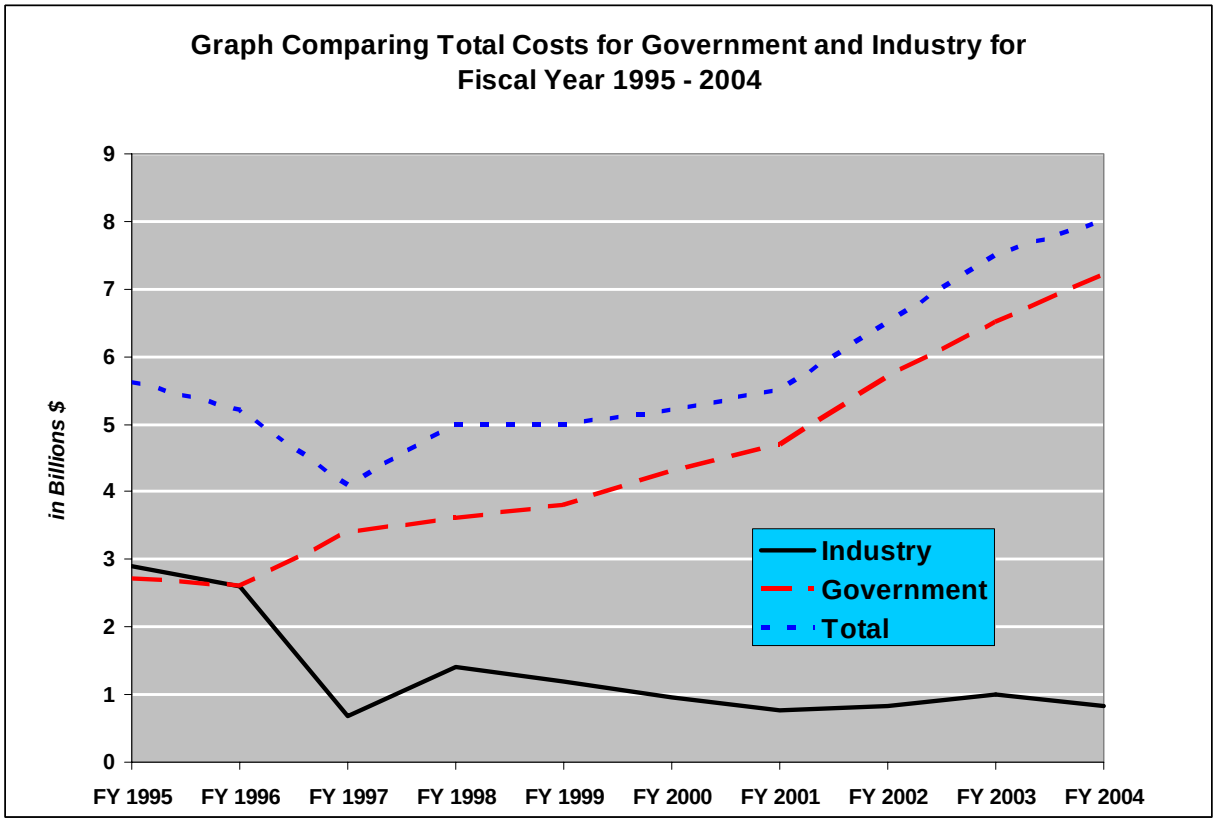
The total security classification cost estimates within Government for FY 2004 is $7.2 billion. This figure represents estimates provided by 41 executive branch agencies, including the Department of Defense, whose estimate incorporates the National Foreign Intelligence Program. It does not include, however, the cost estimates of the Central Intelligence Agency (CIA), which that agency has classified.



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 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 2004 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, 2004, was the end of their fiscal year. The estimate of total security classification costs for 2004 within industry was $823 million.

The Government cost estimates shows an 11 percent increase above the cost estimates reported for FY 2003. The industry numbers are down 18 percent from 2003. This makes the total 2004 cost estimate for Government and industry $8 billion, which is $700 million more than the total cost estimate for Government and industry in 2003. These numbers suggest that post-9/11 increases in security spending, at least as it relates to security classification activity, are beginning to slow. In our FY 2003 report, the total increase was $1 billion, or 14 percent over the FY 2002 figure.



One of the three main drivers of the $700 million total Government increase came from the Physical Security category, which was up $200 million from FY 2003. The other main drivers were Information Technology Security, which was also up by $200 million, and Security Management and Planning, which was up by $242 million. The September 11, 2001 terrorist attacks generated many new physical security requirements. The primary concern behind these new requirements was the protection of employees, but since most of these same employees work in classified environments, the cost of these security enhancements are captured in the ISOO survey since they are serving the dual purpose of protecting both personnel and classified information.

Nevertheless, the fortified homeland defense posture being adopted by many agencies has generated entirely new physical and information technology requirements. Many agencies are installing secure facilities and communications systems that they never had in the past. A number of agencies are still in the process of building Sensitive Compartmented Information

Facilities (SCIFs) and emergency operational control centers. Along with this, many agencies are still dealing with the requirement to establish Continuity of Operations (COOP) sites, which in turn generates the need for more secure facilities and communications. All of these factors account for most of the increases in the three main "drivers" cited above, and the upward trend in these areas will likely continue. Additionally, a new requirement to implement the recently established standards for Personal Identity Verification (PIV) throughout the executive branch by October 2006 will generate more expenditure.

There are benefits derived from these projects and expenditures. For example, one of the main lessons learned from the analysis of business practices utilized prior to the September 2001 terrorist attacks is that information sharing was lacking among the various agencies responsible for protecting the nation. The prime motivation behind the new secure facilities and communications is the rectification of this deficiency. Additionally, many of these new facilities will support emergency responses to a variety of emergencies not related to security classification (e.g. natural disasters).

One encouraging trend is that the increase in Security Management and Planning seems to be driven by more than just the need to plan and manage new physical security programs. Several agencies have mentioned that their senior leadership is now more involved in the areas of security awareness and training, and more attentive to the development of good internal security guidance and regulations. In this same vein, spending on Security Education and Training is up by $19.5 million, or 12 percent, with several agencies reporting that they are using the money to develop quality web-based training tools that will be capable of reaching wider audiences.

For FY 2004, the agencies reported declassification cost estimates of $48.3 million. This figure reflects an 11 percent decrease from FY 2003. As noted in the 2004 ISOO Annual Report, dated March 31, 2005, on the status of the security classification program, the number of pages declassified is down by 34 percent from that reported for FY 2003. This appears to be a continuance of a downward trend since 1997 in both the dollars allocated and the number of pages declassified. ISOO is concerned about the decline in funding because some agencies may be operating under the perception that automatic declassification is a one-time event rather than a process which will continue and require funding for the long term. It is important to emphasize that December 31, 2006 is merely the first automatic declassification deadline. Every year subsequent to 2006, a new body of classified records that is 25 years old and has permanent historical value under title 44, United States Code, will be subject to automatic declassification.

Declassification was not the only category that decreased in FY 2004. Personnel Security experienced a slight decrease of $11 million, or 1 percent. However, this appears to be a temporary respite, since two large agencies are projecting higher outlays in this area in the future. Two main reasons for the projected increase are the continuing expansion of information sharing programs at the state and local levels, which will necessitate access eligibility determinations, and a change in the scope of background investigations, which is part of a reform process precipitated by significant espionage cases.

SUMMARY

Overall, estimated costs to implement the requirements of Executive Order 12958, as amended, and Executive Order 12829, as amended, continue to climb. We believe this is primarily attributable to the continued increased volume of classified information and the ongoing fortification of our nation's critical infrastructure through existing and new protective systems. Clearly, there is a direct correlation between these two attributes. As critical infrastructures are reexamined/initially identified, certain aspects pertinent to vulnerabilities and threats to these structures may require the extraordinary protection of the security classification system. This, in turn, necessitates expenditures for determining individual access eligibility determinations, as well as other costs for handling and safeguarding classified information.