JOINT HEARING BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

AND

SUBCOMMITTEE FOR TECHNOLOGY AND PROCUREMENT POLICY

COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

MAY 2, 2002

H.R. 3844 "FEDERAL INFORMATION AND SECURITY REFORM ACT OF 2002"

STATEMENT FOR THE RECORD

DAVID C. WILLIAMS
INSPECTOR GENERAL
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Mr. Chairmen, and members of the subcommittees, I appreciate the opportunity to appear today to provide an Inspector General's (IG) perspective. Government agencies continue to struggle with the appropriate balance between IT security and computing capacity, too often with an overwhelming bias toward speed and ease of operations. The Government Information Security Reform Act (GISRA) has served as an essential beacon urging agencies toward a more balanced course. During Fiscal Year 2001, the GISRA assessments identified substantial vulnerabilities across government that could threaten the security of information systems. These included:

- Formal security training and awareness programs for all employees were frequently ineffective or non-existent. In the Internal Revenue Service, for example, 70 of 100 employees were willing to compromise their passwords, during pretext telephone calls by IG auditors. No matter how strong other controls may be, employees can often be the most vulnerable component of an agency's IT security program.
- Specific performance measures were often absent, such as the effectiveness of efforts to reduce the impact of computer viruses.
- Oversight of contractors was not sufficient and many had not received the necessary background clearances.
- An unacceptable number of systems and applications critical to the agency missions were not security certified and accredited.

- System intrusion incidents were not consistently reported and shared throughout the government to assist agencies to proactively identify and combat hacking.
- Security controls often seemed to be an afterthought in IT budget and investment decisions, and
- Senior managers often assumed little responsibility for IT security within their programs, deferring entirely to small security offices.

To increase the likelihood of success, agencies need to be held accountable for their security programs. Some agencies have appeared to view the GISRA annual reporting process as a pro forma exercise. To assure GISRA effectiveness, funding requests for IT initiatives should be contingent on the integration of adequate security controls.

- To assist agencies in adhering to GISRA and H.R. 3844 provisions, we offer the following suggestions to improve consistency in conducting and reporting information security assessments and investigations.
- Certain terminology should be clarified to avoid confusion in reporting. Terms such as “programs”, “systems”, “networks”, “mission-critical” and “mission essential” are subject to varying interpretations.
- Agency officials should be required to use the NIST IT security assessment framework.

- Agency and IG reporting requirements should be integrated to reduce duplication of effort.
- The OMB should provide implementation guidance at the beginning of each reporting year.
- Annual submissions should contain a conclusion section on agency compliance with the law and its overall information security posture.
- The IGs should be required to evaluate whether agencies have a process that incorporates information security into their Enterprise Architectures.
- Reporting intrusion incidents to FedCIRC should not be limited to national security incidents, but should also include threats to critical infrastructure, as was the case during the Y2K initiative, and
- Importantly, agencies should identify the IG or another law enforcement organization that will investigate intrusions and refer them for prosecution.

In conclusion, while it is still early in the GISRA implementation process, we are optimistic that, if enforced, the GISRA and its successor legislation will ultimately succeed in strengthening information security throughout the government.

I would be happy to answer any questions.