Policy Directive 710-01 March 21, 2007
Replacement for OIG Manual Chapter 1630

OIG Computer Security

This policy addresses the implementation of an effective computer security and risk management program in the OIG. The OIG follows Treasury Department Policy TD P 85-01.

What does "computer security" include?

It includes policies, procedures, and guidelines that safeguard OIG Information Technology (IT) resources (hardware, software, and data). It outlines cost-effective management, personnel, operational, and technical controls to protect information, ensure integrity, and maintain the availability of IT resources.

What elements make up the OIG computer security program?

A "total" program that ensures adequate security for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

- **Application Security**. Ensuring that information systems incorporate appropriate administrative, and technical safeguards. For sensitive systems, controls include identifying security needs, performing design reviews, conducting system tests, obtaining certification, periodically recertifying, and establishing contingency plans.
- **Personnel Security.** Screening of individuals doing system development life cycle work or accessing sensitive data. Assigning of security officials. Reviewing, revoking, and authorizing privileges for users.
- **Physical Security**. Controlling access to our building, work areas and equipment. Conducting periodic risk assessments, obtaining certification, and developing disaster recovery and continuity of operations plans.
- **Security Awareness and Training Programs**. Providing annual security awareness training to all employees and staff involved in the management, development, or use of information systems. Providing annual specialized security training to all IT and designated OIG staff members.

What general guidelines do computer users need to follow?

- Position monitors and printers so that others cannot easily see their screens and printouts.
- Use electrical surge protectors to protect computers equipment.
- Read and follow the safety and security precautions/instructions for hardware, software, and/or services that will be used.
- Stay alert for viruses. Unexplained screen displays, slow software and data access, or mysteriously disappearing software or files may indicate a virus on your computer.
- Scan all media from outside the OIG (e.g., from home or other agencies) for viruses before their use. If you detect a virus, take the disk out of your computer and report the incident to the Office of Management, Information Technology Division (ITD).
- Only leave computers, printers, disks, tapes, and data at work sites with a responsible person or in a locked room.
- Backup data regularly onto disks, CDs, thumb drives, or to a network drive for backup to network tapes.
- Abide by applicable guidance regarding use of OIG Information Technology resources.
- Be aware of the security category of data you are handling, do not process or store classified information on unclassified systems.

Who is responsible for Computer Security?

The ITD Director, ISSO, senior managers, IT liaisons, and employees all have computer security responsibilities.

The Assistant Inspector General for Management (AIGM) has overall responsibility for OIG computer security and risk management, serves as the Senior Information Resources Management Official (SIRMO), and appoints the OIG Information System Security Officer (ISSO).

- **The ITD Director** manages the Computer Security and Risk Management program for the AIGM.
  - Represents the OIG at Department of the Treasury security meetings.

  - Evaluates IT products' security features for OIG applicability.
  - Develops and implements hardware/software configuration management procedures.
  - Corrects deficiencies identified in risk assessments, reviews, inspections, and audits.
  - Oversees protective and corrective actions on reported security incidents.

- **The ISSO** records and investigates reported security incidents and notifies appropriate personnel.
  - Maintains IT security plans, risk assessments, disaster contingency plans, security incident reports, security training rosters, etc.
  - Maintains passwords and electronic keys created for critical/privileged accesses to facilities, devices, systems, applications, files and localized computer processes.
  - Prepares and coordinates IT security training and awareness for the OIG.
  - Assists OIG employees and IT contractors with IT security related issues.

- **Senior managers** are responsible for security in their work area.
  - Appoint a primary and alternate IT Liaison for his/her work area.
  - Safeguard IT resources and telecommunication assets under his/her management control.
  - When necessary, take protective and/or corrective actions on reported security incidents or observed irregularities.

- **IT Liaisons** work with their senior managers and the ISSO to ensure their work areas satisfy the guidelines in this policy.
  - Help test and implement security procedures to control access to IT resources.
  - Investigate reported security incidents and any protective and/or corrective actions taken to his/her Senior Manager.
  - Provide security awareness and training to employees as requested. Assist employees and contractors working in their area.

- **Employees, student interns, and contractors**
  - Protect IT resources and information from loss, theft, misuse, and unauthorized changes.
  - Protect passwords and electronic keys from unauthorized disclosure.
  - Access only the IT resources and information specifically authorized.
  - Protect SBU information. If the sensitivity of any information is in doubt, ask management for clarification.
  - Report promptly any seen or suspected security incidents.

How do I report a security incident?

If you see or suspect a compromise of information on our network, or a loss or theft of IT resources, please email the IT HelpDesk at Helpdesk@oig.treas.gov. We will record all facts and actions on a Security Incident Report within 5 hours of an incident's initial reporting, if possible. The ISSO will investigate security incidents and recommend protective and/or corrective actions to the ITD Director. The ITD Director will determine follow-up actions and record them onto his/her copy of the Security Incident Report. If appropriate, the ISSO or the ITD Director will contact or ask a field manager to contact local federal or local law enforcement officers.

If I have a question about this policy, whom can I contact?

Please contact the Office of Management by email at OIG-OM@oig.treas.gov or call our main line at (202) 927-5200.