# TREASURY DIRECTIVE: 85-03

**DATEDATE**: January 9, 2009

**ADMINISTRATIVE EDIT:** August 9, 2016

**SUBJECT:** Authorities of the Departmental Chief Information Officer to Respond to Information Technology (IT) Security Incidents, Threats, and Vulnerabilities

1. **PURPOSE.** This directive describes the authorities of the Deputy Assistant Secretary for Information Systems and Chief Information Officer (DASIS/CIO) in the event of an IT security incident or identification of a significant IT security vulnerability.

2. **SCOPE AND APPLICABILITY.**

   a. This directive applies to all information technology systems operated by or on behalf of the Department and its bureaus, offices, and related organizations. This scope includes systems within the Departmental Offices, Department-wide systems operated under the purview of the DASIS/CIO, and systems operated by or on behalf of the Departmental bureaus.

   a. The authority of the Inspectors General is set forth in Section 3 of the Inspector General Act and the Internal Revenue Service Restructuring and Reform Act, and defined in Treasury Order 114-01 (OIG) and Treasury Order 115-01 (TIGTA), or successor orders. The provisions of this directive shall not be construed to interfere with that authority.

   a. Those authorities reserved to the Assistant Secretary (Intelligence and Analysis) concerning United States intelligence activities are not affected by this directive.

3. **POLICY.**

   a. The Department and its bureaus shall establish and maintain the capability to respond to computer or network based security incidents and threats in order to preserve the ability to perform necessary government functions, protect Treasury information and information system assets, and maintain the confidentiality and integrity of business and personal information under the custody of Treasury.

   a. The DASIS/CIO shall serve as the overall Departmental authority for the secure operation of Department IT resources.

   a. As such, the DASIS/CIO is authorized to take necessary and appropriate action(s) in response to an actual, suspected, or threatened IT security incident or significant IT vulnerability.

   a. Prior to taking any action authorized under this directive, the DASIS/CIO shall coordinate such actions with bureau management officials and other responsible security officials within the Department. As part of this coordination, the DASIS/CIO shall brief bureau officials on information on threats and vulnerabilities. Additionally, the DASIS/CIO shall notify appropriate bureau officials prior to providing information to parties outside the Department about bureau incidents, vulnerabilities, or related sensitive bureau information.

4. **DEFINITIONS.**

   a. IT Security Incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that could result in the inability of the Department to continue to perform necessary business functions, the disclosure of sensitive or classified Treasury information, or the loss of confidentiality or integrity of business or personal information under the Department's custody. An "imminent threat of violation" refers to a situation in which there is a factual basis for believing that a specific incident is about to occur. (For example, antivirus software maintainers may receive a bulletin from the software vendor, warning them of a new worm that is rapidly spreading across the Internet.)

   b. Significant IT Vulnerability is one or more weaknesses or deficiencies in the security of Department computer systems or networks, identified by an authoritative source (e.g., product provider, U.S. Government agency, etc.,) that if unaddressed could lead to an IT Security Incident.

   c. Necessary and Appropriate Actions are coordinated management decisions or other measures, both precautionary and reactive, to address known or suspected IT security incidents, events, threats, and vulnerabilities.

5. **RESPONSIBILITIES.**

a. The DASIS/CIO shall, in coordination with bureau management officials and other responsible security officials within the Department, assess the particular circumstances of an incident or vulnerability (in particular the severity or criticality of the event), determine the appropriate action to be taken, and communicate those decisions as appropriate.

b. Bureau executives and IT management officials shall work cooperatively with the DASIS/CIO to implement all coordinated actions necessary to address IT security incidents or significant IT security vulnerabilities.

6. **AUTHORITIES.**

a. Public Law 107-347, "E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) of 2002," December 17, 2002.

b. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources."

c. National Security Directive (NSD) 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990, CONFIDENTIAL.

d. Public Law 104-106, "Clinger-Cohen Act of 1996" [formally called Information Technology Management Reform Act (ITMRA)], February 10, 1996.

e. Privacy Act of 1974, as amended, 5 USC 552a, Public Law 93-579, July 14, 1987.

f. EO 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001.

g. Homeland Security Presidential Directive (HSPD) #7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

h. Department of State 12 Foreign Affairs Manual (FAM) 600, "Information Security Technology."

i. Treasury Directive Publication 85-01, "Treasury Information Technology Security Program."

j. Treasury Order 102-10, "Designation of Chief Information Officer for the Department of the Treasury."

k. Treasury Order 101-05, "Reporting Relationships and Supervision of Officials, Offices and Bureaus, and Delegation of Certain Authority in the Department of the Treasury."

7. **OFFICE OF PRIMARY INTEREST.** Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer, Office of the Assistant Secretary for Management.

/S/
Peter B. McCarthy
Assistant Secretary for Management
and Chief Financial Officer