TREASURY DIRECTIVE: 85-01

DATE: March 10, 2008

SUBJECT: Department of the Treasury Information Technology (IT) Security Program

1. PURPOSE. This Directive authorizes the issuance of Treasury Department Publication (TD P) 85-01, "Treasury IT Security Program," which contains Department-wide IT security requirements and supporting guidance.

2. POLICY.

All IT systems operated by or on behalf of the Department of the Treasury shall be adequately protected to ensure confidentiality, integrity and availability in order to minimize the risk of
unauthorized access, use, disclosure, disruption, modification or destruction.

b. The Treasury IT Security Program (TD P 85-01) shall define controls for providing such protection. The Chief Information Officer (CIO) is authorized to prescribe, publish and maintain TD P 85-01, which is issued as a separate document. It shall:

(1) set forth the minimum standards or requirements for the security of non-national security and national security IT systems and the information they process, store and communicate;

(2) provide uniform policies and standards (and when appropriate, general procedures) to be used by the bureaus to address their IT security responsibilities in accordance with applicable requirements issued by the Department, Office of Management and Budget, Department of Defense, National Security Agency, General Services Administration, Government Accountability Office, Department of Commerce, Department of Homeland Security and National Institute of Standards and Technology; and

(3) implement and supplement, where necessary, Executive Orders, National Security directives, and other Government regulations by providing guidance when such regulations are not sufficiently detailed, or details are left to Departmental discretion.

3. SCOPE AND APPLICABILITY.

a. This Directive applies to all bureaus, offices and organizations in the Department of the Treasury. The policy applies to all Treasury employees including detailees, temporary employees, and interns and contractors performing work for the Department of the Treasury, its offices, and bureaus working on behalf of the Department whether in a government office, traveling, alternate work site or other location. The requirements in TD P 85-01 apply to all Departmental systems, including those operated by other organizations on behalf of the Department.

b. 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.

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

d. The Treasury IT Security Program does not preclude a bureau or office from applying more stringent internal requirements when appropriate, so long as these are consistent with TD P 85-01.

4. DEFINITIONS

a. Confidentiality – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information

b. Integrity – guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity

c. Availability – ensuring timely and reliable access to and use of information

5. RESPONSIBILITIES.

a. The Deputy Assistant Secretary for Information Systems and Chief Information Officer shall:

(1) oversee the creation and ensure the maintenance of an enterprise-wide IT Security Program;

(2) promote the promulgation of processes and procedures which mitigate the risks to information captured, processed, or maintained by the Department;

(3) ensure Treasury's compliance with the Federal Information Security Management Act;

(4) maintain TD P 85-01 and formally coordinate any changes thereto with the Office of the General Counsel and Treasury Bureaus for review and comment prior to issuance; and

(5) retain discretion to review and approve bureau issuances that implement and supplement the Treasury IT Security Program.

b. The Heads of Bureaus and Offices and the Deputy Assistant Secretary for Headquarters Operations shall:

(1) ensure that an IT security program is implemented within their organizations in accordance with TD P 85-01;

(2) refer to the policies and procedures set forth in TD P 15-71, the Treasury Security Manual, regarding matters covered therein; and

(3) submit new or revised bureau security directives, regulations or handbooks that implement or supplement TD P 85-01 to the CIO for review and approval prior to publication as the CIO may require. No issuance upon which CIO review is invoked shall be published, implemented, adopted or used until approved.

c. The Bureau Chief Information Officers shall designate a point of contact to coordinate all policy issues related to information systems security (including IT security, operational security (threats/vulnerability assessments), emissions security (TEMPEST), certificate management, electronic authentication, continuity planning, and critical infrastructure protection).

6. SUPPLY OF TREASURY IT SECURITY PROGRAM. The text of TD P 85-01 may be accessed from the Department of the Treasury Intranet IT security link.

7. 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 (U), 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, Washington, DC, July 14, 1987.

f. Executive Order (E.O.) 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.

8. CANCELLATION. Treasury Directive 85-01, Department of the Treasury Information Technology (IT) Security Program, dated February 13, 2003, is superseded.

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

/S/

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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu