



**MEMORANDUM OF UNDERSTANDING**  
**Between**  
**Mission Assurance and Security Services' (MA&SS)**  
**Computer Security Incident Response Center (CSIRC)**  
**and**  
**Treasury Inspector General for Tax Administration Office of**  
**Investigations (TIGTA OI)**

**Purpose:** The purpose of this Memorandum of Understanding (MOU) is to identify roles and responsibilities of the Computer Security Incident Response Center (CSIRC) and Treasury Inspector General for Tax Administration Office of Investigations (TIGTA OI) in the reporting and documenting of computer security incidents involving the "Loss or Theft of IT Asset."

**Background:** The Department of Homeland Security operates the US Computer Emergency Response Team (US-CERT) which actively assesses the near to real-time security posture of the nation's cyber assets. Office of Management and Budget (OMB) Memorandum M-06-15 issued May 22, 2006 mandates the reporting of computer security incidents to the US-CERT within the prescribed timeframes based on incident category which includes a 1-hour reporting timeline for "Category 1" incidents.

Consistent with the guidance of Treasury Directive Publication (TD P) 85-01 Volume II, Part 1 Section 6, Incident Response Procedures, the Department of the Treasury Computer Security Incident Response Center (TCSIRC) serves as the central point of contact for escalating incidents reported by Bureau cyber security teams. The TCSIRC facilitates incident reporting with external reporting entities, to include reporting to US-CERT.

**Scope:** The scope of this MOU is limited to only include a computer security incident type that is "Loss or Theft of IT Asset," which is further defined in Table 1 with an associated reporting timeline and category.

Significant Incident Type	Description	IRS CSIRC Reporting Time	Treasury CSIRC Incident Type & Reporting Time	Treasury Category
Loss or Theft of IT Asset	Any incident involving loss or theft of an IT asset (e.g., desktop computer, laptop computer, server, blackberry, CD/DVD, flash drive, floppy, other portable media) that could result in unauthorized access to systems or information.	Reported to IRS CSIRC and first-line manager immediately upon detection, not to exceed 1-hour. Must also be reported to local TIGTA OI.	<b>Unauthorized Access</b> Reported to TCSIRC within 1-hour of detection with recurring updates at 4-hour intervals until resolved.	1

**TABLE 1: Incident Reporting Requirement for "Loss or Theft of IT Asset"**



**Responsibilities:** Each Internal Revenue Service (IRS) employee and organization plays a very important role in ensuring the IRS meets the stringent timelines established by OMB and the US-CERT for computer security incident reporting. It is therefore imperative that ALL computer security incidents identified shall be reported immediately and directly to CSIRC and the first-line managers. In addition, ANY incident involving the "Loss or Theft of IT Asset" that could result in unauthorized access to IRS systems or information MUST also be immediately reported to the local Treasury Inspector General for Tax Administration Office of Investigations (TIGTA OI).

The section below defines the responsibilities of CSIRC and TIGTA OI:

**CSIRC:**

1. Shall track all reports of computer security incidents and document within the Incident Tracking System (ITS), assigning a CSIRC Incident Record number.
2. Shall provide automated notification to TIGTA OI for received incidents involving the "Loss or Theft of IT Asset" using e-mail communications, addressed to the TIGTA Data Analysis Team (DAT) at [DAT@tigta.treas.gov](mailto:DAT@tigta.treas.gov).  
Notification will be provided automatically upon submission to CSIRC ITS and assignment of CSIRC Incident Record Number.
3. Shall collaborate with TIGTA OI to correlate and cross-reference incidents involving "Loss or Theft of IT Asset."
  - a. Shall cross-reference incident reports received from TIGTA OI with CSIRC incidents involving "Loss or Theft of IT Asset" to ensure incidents are properly documented.
  - b. Shall perform monthly reconciliation of incident reports received from TIGTA OI with CSIRC incidents involving "Loss or Theft of IT Asset" to ensure incidents are properly documented.

**TIGTA OI:**

1. Shall track all reports of computer security incidents involving "Loss or Theft of IT Asset" and document the incidents within the Performance and Results Information System (PARIS) by assigning a TIGTA OI complaint number.
2. Shall provide automated notification to CSIRC for received incidents involving the "Loss or Theft of IT Asset" using e-mail communications, addressed to [CSIRC@csirc.irs.gov](mailto:CSIRC@csirc.irs.gov).  
Notification will be provided automatically upon submission to PARIS and assignment of a TIGTA Complaint Number.
3. Shall collaborate with CSIRC to correlate and cross-reference incidents involving "Loss or Theft of IT Asset."
  - a. Shall perform monthly reconciliation of incident reports received from CSIRC with TIGTA OI incidents involving "Loss or Theft of IT Asset" to ensure incidents are properly documented.



### CONTACT INFORMATION:

Name	Title	E-mail Address	Phone	After-hours
Carlos L. Edwards	Incident Response Lead	<a href="mailto:Carlos.L.Edwards@csirc.irs.gov">Carlos.L.Edwards@csirc.irs.gov</a>	202-283-4813	202-316-8801
CSIRC Operations	24x7 CSIRC Ops	<a href="mailto:CSIRCCii@csirc.irs.gov">CSIRCCii@csirc.irs.gov</a> <a href="http://www.csirc.web.irs.gov/incident/">http://www.csirc.web.irs.gov/incident/</a>	866-216-4809	866-216-4809

TABLE-2 CSIRC Contacts

Name	Title	E-mail Address	Phone	After-hours
Thomas Traxinger	ASAC, Data Analysis Team	<a href="mailto:Thomas.Traxinger@tigta.treas.gov">Thomas.Traxinger@tigta.treas.gov</a>	202-927-7201	202-345-5494
TIGTA Field Offices	Special Agents-in-Charge (SAC)	<a href="mailto:DAT@tigta.treas.gov">DAT@tigta.treas.gov</a> <a href="http://www.treas.gov/tigta/about_office.shtml/">http://www.treas.gov/tigta/about_office.shtml/</a>	800-366-4484	800-366-4484


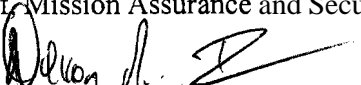
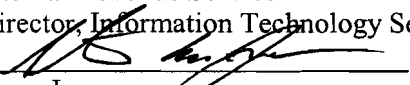
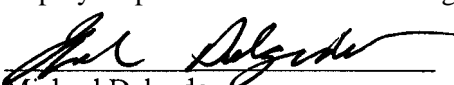
TABLE3 TIGTA OI Contacts

### EFFECTIVE DATE

This Memorandum of Understanding becomes effective on the date of the last signature, and may be terminated at any time, by mutual consent of the Points of Contact.

**MOU NUMBER: MOU-CSIRC-20061215-001**

### SIGNATURES

 _____ Daniel Galik Internal Revenue Service Chief, Mission Assurance and Security Services	<u>12/7/06</u> Date
 _____ Devon Bryan Internal Revenue Service Director, Information Technology Security	<u>12/5/06</u> Date
 _____ Steve Jones Treasury Inspector General for Tax Administration Deputy Inspector General for Investigations, Office of Investigations	<u>12/28/2006</u> Date
 _____ Michael Delgado Treasury Inspector General for Tax Administration Assistant Inspector General for Investigations, Office of Investigations	<u>12/21/06</u> Date