



IT Security Handbook

Incident Response and Management: Targeted Collection of Electronic Data

ITS-HBK-2810.09-03
Effective Date: 20110824
Expiration Date: 20130824
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.09-03)
Incident Response and Management: Targeted Collection of Electronic Data

Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

ITS Handbook (ITS-HBK-2810.09-03)
Incident Response and Management: Targeted Collection of Electronic Data

Change History

Version	Date	Change Description
1.0	08/24/2011	Change from ITS-SOP-0008 to ITS-HBK-2810.09-03. Revise and update SOP language.

ITS Handbook (ITS-HBK-2810.09-03)
Incident Response and Management: Targeted Collection of Electronic Data

Table of Contents

1.0	Introduction and Background.....	5
2.0	Roles and Responsibilities	5
3.0	Process	8
	Appendix A. Definitions.....	11
	Appendix B. Acronyms	12
	Appendix C. Forms	13

1.0 Introduction and Background

- 1.1 This Information Technology (IT) Security Handbook (ITS-HBK) establishes the processes for initiating, managing, and ending the collection and analysis of NASA electronic data in support of the investigation of NASA users. For the purpose of this handbook, Targeted Collection of Electronic Data (TCED) is defined as the collection and analysis of data in an electronic form in order to provide information about a NASA user's use of NASA information system resources due to suspected inappropriate, illegal, criminal, or intentional harmful use of NASA's information systems and resources. This handbook supports implementation of requirements in *NASA Procedural Requirement (NPR) 2810.1, Security of Information Technology*.
- 1.2 **Scope:** The processes in this handbook apply to all requests to initiate collection and conduct analysis of data from NASA information systems for the purposes of supporting administrative or criminal investigations as outlined in *NPR 2810.1*. This handbook does not cover telecommunications data such as telephone communications, telephone records, and Voice over Internet Protocol (VoIP) transmissions. Additionally, this policy does not apply to routine traffic and network monitoring or incident response activities detailed in *ITS-HBK-2810.09-02, Incident Management: NASA Information Security Incident Management*.
- 1.3 **Purpose:** The purpose of this handbook is to:
- Ensure that the performance of a TCED is fair and consistent throughout NASA.
 - Prevent the misuse of a TCED.
 - Ensure due diligence when requesting and performing a TCED.

Applicable Documents

- *NPR 1441.1D, NASA Record Retention Schedules*
- *NPR 1600.1, NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)*
- *NPD 2540.1G, Personal use of Government office Equipment Including Information Technology*
- *NPR 2810.1, Security of Information Technology*
- *ITS-HBK-2810.09-02, Incident Management: NASA Information Security Incident Management*

2.0 Roles and Responsibilities

The NASA Chief Information Officer (CIO) shall:

- Inform NASA Senior Management of a TCED, as appropriate.
- Delegate to the Senior Agency Information Security Officer (SAISO) the responsibility and accountability for the NASA-wide implementation of the NASA Incident Response and Management: TCED handbook processes.

The Center CIO shall:

- Inform the Center Director of TCED activity and findings, as appropriate.
- Maintain a technical capability to support a reasonable number of TCED requests.
- Negotiate with requesting parties when resource constraints are identified in supporting a TCED.

The Senior Agency Information Security Officer (SAISO)

The SAISO shall:

- Maintain responsibility and accountability for the NASA-wide implementation of the NASA TCED policies and processes.
- Inform the NASA CIO about TCED activities and findings, as appropriate.
- Provide for agency level resources to support TCED activities, when requested.

The SAISO may:

- Receive requests to initiate a TCED.

The Information Technology Security Manager (ITSM)

The ITSM shall:

- Submit TCED requests to the appropriate vetting authorities for identified misuse activity.
- Review and assign resources for TCED requests from authorized NASA managers and law enforcement officials.
- Obtain a TCED case number from the Security Operations Center (SOC).
- Review the information security staff's report on anomalous or suspicious network traffic, follow incident handling and response procedures, and determine if a TCED is necessary.
- Maintain documentation of all TCED activities involving the Center, including law enforcement or other requests for a TCED and receipts for TCED records.
- Ensure all data collected from monitoring is properly safeguarded.
- Inform Center CIO, SAISO, or NASA managers on the results of a TCED, as appropriate.
- Notify the SAISO or Information System Owner (ISO) of TCED requests, as appropriate.

The ITSM may:

- Receive requests to initiate a TCED.
- Delegate their responsibilities as appropriate.

The Information System Owner (ISO):

The ISO shall:

- Submit requests for initiation of a TCED to the relevant parties when targeting the activities of NASA Users on information systems under their authority.
- Support duly vetted TCED requests.
- Notify the SAISO or ITSM of TCED requests, as appropriate.
- Obtain a TCED case number from the ITSM or SOC.
- Arrange for resources capable of supporting a TCED.
- Negotiate with requesting parties when resource constraints are identified in supporting a TCED.
- Inform SAISO, ITSM, or NASA managers on the results of the TCEDs, as appropriate.

The ISO may:

- Receive requests to initiate a TCED.
- Request technical support from the OCIO or Center CIOs in responding to a TCED requests.
- Delegate to the Information System Security Official (ISSO) the support of a TCED.

The Security Operations Center (SOC) Operations Manager shall:

- Direct all TCEDs to the SAISO or responsible ITSM, as appropriate.
- Assign a TCED case number to all TCED requests.

The NASA Civil Service Supervisor shall:

- Submit initiation requests to the Center's Human Resources Employee Relations Specialist in consultation with the Office of the General Counsel (OGC), or the Center Office of the Chief Counsel (OCC) if applicable, in order to monitor a civil service employee's use of NASA computer equipment or resources for suspected misuse.

The Contracting Officer shall:

- Submit TCED initiation request to the Center OCC or OGC, as appropriate, in order to investigate a contract employee's use of NASA computer equipment or resources for suspected misuse.
- Engage the Contracting Officer Technical Representative (COTR), as appropriate.
- Request the OCC or OGC make a formal request to initiate a TCED of contract employees.

Individual supporting TCED shall:

- Sign a non-disclosure agreement, as appropriate.
- Provide technical support and monitoring services for an authorized TCED.

ITS Handbook (ITS-HBK-2810.09-03)
Incident Response and Management: Targeted Collection of Electronic Data

- Inform the SAISO, ITSM, or ISO on the progress and results of a TCED, as appropriate.
- Provide results of TCED activities to parties identified in the TCED request.
- Properly safeguard all data collected while conducting a TCED.

The Office of the Inspector General (OIG)

The OIG shall:

- Review and validate all requests for a TCED from the OIG to ensure they meet legal and administrative requirements.
- Negotiate with supporting parties when resource constraints are identified in supporting a TCED.
- Submit properly vetted requests to the SAISO, ITSM, or ISO when requesting support for a TCED.

The OIG may:

- Request technical assistance in performing a TCED, when applicable.

The Deputy Assistant Administrator for the Office of Protective Services (OPS):

The Deputy Assistant Administrator for OPS shall:

- Review and validate all requests for a TCED from OPS to ensure they meet legal and administrative requirements.
- Negotiate with supporting parties when resource constraints are identified in supporting a TCED.

The Deputy Assistant Administrator for OPS may:

- Formally request NASA to perform a TCED during the course of a counter-intelligence (CI) investigation or other OPS investigation.

The Office of the General Counsel (OGC)/ Office of the Chief Counsel (OCC):

The OGC/OCC shall:

- Review requests from contractor managers.
- Request a TCED on behalf of contractor managers.

The OGC/OCC may:

- Upon Office of Human Resources (OHR) request, assist OHR in the determination of whether to make a formal request for a TCED.
- Submit request for the initiation of a TCED in support of court orders or other legal actions.

The Center Human Resources Employee Relations Specialist (Office of Human Resources or Office of Human Capital Management (OHCM)) shall:

- Review requests from supervisors for a TCED and request help from the OGC or the OCC in evaluating those requests.

3.0 Process

3.1 Requirements

- 3.1.1 A TCED shall be conducted only under the appropriate authority as granted by a legal statute or policy.
- 3.1.2 A TCED may be justified for any of the following reasons:
 - A violation of NASA policy
 - A court order
 - A signed request from any of the following:
 - (1) OIG
 - (2) OGC
 - (3) OPS
 - (4) OHCM
 - (5) OHR
 - (6) OCC
- 3.1.3 All TCED activities must follow the processes set forth in this handbook.
- 3.1.4 No TCED shall be conducted without appropriate vetting and approval as set forth in this handbook.
- 3.1.5 A TCED request may apply to available existing data, such as saved logs, archived network traffic, or the contents of storage media.
- 3.1.6 A TCED request may involve the collection and analysis of data not previously collected.
- 3.1.7 The end date of such a TCED shall not be later than three months after the start date.
- 3.1.8 The requestor may submit a request to extend the TCED for an additional three-month period after the initial period expires. Only one request to extend shall be considered for each TCED case number.
- 3.1.9 The individual supporting the TCED shall consider all data related to the TCED as sensitive information (e.g. Sensitive But Unclassified (SBU), Controlled Unclassified Information (CUI), etc.), and apply all protections required for sensitive information while handling and storing this data.
- 3.1.10 Additional handling requirements may be imposed by the requestor or due to heightened sensitivity of the data. The individual supporting the TCED shall follow, within reason, any specific data handling and storage procedures that the requestor requires.

3.2 Initiating a Targeted Collection of Electronic Data

- 3.2.1 Submit a signed *Request for Targeted Collection of Electronic Data form* (*Appendix C*) to the SAISO, ITSM, or ISO (recipient) as is appropriate to the TCED.
 - If the recipient of the TCED request is an ISO, they shall obtain a TCED case number from the ITSM or SOC.
 - TCED requests shall include as much detail as possible (without compromising an investigation or disclosing sensitive information) so that the activity can be sufficiently focused and effective.
 - The TCED requests shall specify the collection, monitoring, review and analysis requirements (for example, all incoming and outgoing activity to or from a given IP address(es), all traffic on specified ports, all traffic about specified information), including:
 - 1. Any special requirements for data storage and handling;
 - 2. Parties to be notified; and,
 - 3. Methods of communicating results.

- 3.2.2 A TCED case number shall be assigned by the SOC and made available to both the requestor of the TCED and the recipient of the TCED request to assure consistent tracking.
- 3.2.3 The recipient of the TCED request shall identify any resource constraints and work with the requestor to build an acceptable management plan.
- 3.2.4 Before proceeding with the TCED, the recipient of the TCED request shall ensure:
- The *Request for Targeted Collection of Electronic Data* form in the Appendix C is completed in full;
 - The authority under which the proposed monitoring will take place is clear;
 - The request is clear and unambiguous;
 - The organization can support the requested action;
 - The appropriate management has been made aware of the TCED; and,
 - The resources and needed data sources to support the request have been identified.
- 3.2.5 No TCED activity shall be requested and validated by the same person.
- 3.2.6 The SAISO or responsible ITSM, as appropriate, shall retain the signed request form on file.

NOTE: These processes refer only to requesting, initiating, managing, and ending an actual TCED, once an official requestor has determined that a TCED is needed. The processes do not include any initial review by OHR or other preliminary evaluation of whether a TCED should occur.

3.3 Managing a Targeted Collection of Electronic Data

The recipient of the TCED request, in consultation with the appropriate personnel and in coordination with the requestor of the TCED, shall develop and manage a TCED management plan that includes:

- a. When and how often the individual supporting the TCED reports results and to whom.
 - b. What kind of data, if found, is collected and delivered.
 - c. The media, format, and delivery method for the TCED results.
 - d. How long the individual supporting the TCED will retain the results after delivering them to the requestor, if applicable.
- 3.3.1 The individual supporting the TCED shall carry out the collection, monitoring, review and analysis as agreed and authorized.¹
- 3.3.2 The results shall be submitted to the recipient of the TCED request for review upon completion of the TCED and before delivery to the requestor.
- If the ISO is the recipient of the TCED request, the ISO shall communicate the completion of the TCED to the SAISO or ITSM as appropriate.
- 3.3.3 The results shall then be submitted to the requestor.
- During a TCED, the requestor may ask for interim results from the monitoring. Multiple receipts may be necessary as data may be provided to the requestor on multiple occasions during the course of the TCED activity. All receipts shall be maintained by the SAISO or ITSM, as appropriate.
- 3.3.4 Upon receipt of the TCED results, the requestor shall sign a receipt acknowledging that the monitoring was conducted and that they received the requested materials. The form *Receipt of Targeted Collection of Electronic Data Records (Appendix C)* shall be used.

¹ **NOTE:** The requestor may require the individuals supporting the TCED to sign a non-disclosure agreement, if applicable.

3.4 Ending a Targeted Collection of Electronic Data

- 3.4.1 When the collection period ends, or at a time agreed upon by the requestor of the TCED, the results shall be delivered to the requestor of the TCED or the point of contact specified in the request.
- If the recipient of the TCED request was an ISO, they shall inform the SAISO or responsible ITSM as to the delivery of the requested data and provide the signed receipt(s).
- 3.4.2 Upon receipt of the results, the requestor shall sign the receipt form, *Receipt of Targeted Collection of Electronic Data Records (Appendix C)*, acknowledging that monitoring results were received and that the TCED is complete.
- If data was sent to the requestor of the TCED on several occasions during the course of the monitoring activity, the requestor of the TCED shall submit a receipt for each occasion.
 - All receipts shall be maintained by the SAISO or responsible ITSM for a minimum of three years.
- 3.4.3 It is the requestor's responsibility to verify that they received the complete results in a readable format. If necessary, the requestor of the TCED may ask for technical assistance from the recipient of a TCED or the individual supporting the TCED.
- 3.4.4 Upon receipt of the TCED results, the requestor of the TCED shall assume all responsibility for the information.

3.5 Handling and Storing the Resulting Data

- 3.5.1 When a TCED is related to a criminal or counter-intelligence investigation, it may be necessary to follow special procedures for handling and storing the monitoring results to preserve legal evidence or to protect sensitive information. If there are such requirements, the requestor shall give the monitoring staff any additional training and assistance that they need.
- 3.5.2 The individual supporting the TCED shall follow, within reason, any specific data-handling and storage procedures that the requestor requires. The individual supporting the TCED shall also keep all details of any TCED confidential, and they may be required to sign a non-disclosure agreement. Any information that results from or is related to a TCED shall only be transmitted using NASA-standard encryption, fax, mail, or hand-delivery.
- 3.5.3 The individual supporting the TCED is not required by this handbook to retain the results; however, they may retain copies to comply with Center retention policies, to assist the requestor as previously agreed, or to follow instructions from the SAISO, ITSM, or ISO. When the individual supporting the TCED deletes the results, they shall follow the *NPR 1600.1* requirements for destroying sensitive information.
- 3.5.4 The individual who receives the TCED results (such as requestors of the TCED or their designated points of contact) shall also handle, store, and dispose of monitoring data in accordance with all applicable NASA and Federal policies. This includes, for example, destroying the data from TCED that found no actionable activity.
- 3.5.5 The SAISO or ITSM shall retain all requests for a TCED for a minimum of three years. The SAISO or ITSM shall also retain all receipts for the results of a TCED delivered to the requestor for a minimum of three years. TCED information may contain sensitive information and should be handled, stored in accordance with NASA requirements for sensitive information (e.g. for SBU *NPR 1600.1*).

Appendix A. Definitions

Counter-Intelligence	The term "counter-intelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities [50 USC 401a].
Information System	A discrete set of resources designed and implemented for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NPR 2810.1B)
Internet Protocol (IP)	A standard designed for use in interconnected systems of packet-switched computer communication networks. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fix-length addresses.
NASA User	Any explicitly authorized patron, civil servant or contractor, of a NASA information system.
Routine monitoring	Capturing, reviewing, and inspecting electronic data to improving IT services, protect NASA networks and systems, and ensure compliance with NASA policies.
Standard Operating Procedure	Instructions for carrying out an official NASA process or procedure
Sensitive But Unclassified	Unclassified information that does not meet the standard for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interest of the United States or originated by entities outside the U.S. Federal government, and under law or policy requires protection from disclosure, special handling safeguards, and prescribed limits on exchange or dissemination.
Targeted Collection of Electronic Data (TCED)	The specific or prolonged monitoring of electronic data that is linked to specific people, IP addresses, or equipment.
Voice over IP	A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone. (Wikipedia)

Appendix B. Acronyms

CI	Counter-Intelligence
CIO	Chief Information Officer
CO	Contracting Officer
COTR	Contracting Officer Technical Representative
CUI	Controlled Unclassified Information
IP	Internet Protocol
ISO	Information System Owner
ISSO	Information System Security Official
IT	Information technology
ITS-HBK	Information Technology Security Handbook
ITSM	Information Technology Security Manager
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCC	Office of the Chief Counsel
OGC	Office of the General Counsel
OHCM	The Office of Human Capital Management
OHR	Office of Human Resources
OIG	Office of the Inspector General
OPS	Office of Protective Services
SAISO	Senior Agency Information Security Officer
SOC	Security Operations Center
SOP	Standard Operating Procedure
SBU	Sensitive But Unclassified
TCED	Targeted Collection of Electronic Data
VoIP	Voice over IP

Appendix C. Forms

Request for Targeted Collection of Electronic Data

Note: All fields in **bold** are required.

Date of Request:	Secure Data Exchange: <input type="checkbox"/> Entrust <input type="checkbox"/> PGP or <input type="checkbox"/> Other	
Requestor (name, title, organization, Center):	Contact Information Phone: Fax: E-mail:	
Signature:	Date:	
Other Approved POCs:		
Requestor Case or Activity Number:	Requested start date	End Date (3 months or less):
<input type="checkbox"/> Routine Monitoring Found Anomalous or Suspicious Activity <input type="checkbox"/> Office of the Inspector General <input type="checkbox"/> Human Capital Management <input type="checkbox"/> General Counsel <input type="checkbox"/> Counter-Intelligence <input type="checkbox"/> Criminal <input type="checkbox"/> other: _____		
Target Description (subject names if applicable, system IP, domain information):		
Specific Monitoring, Storage, and Handling Requirements (such as: monitor all incoming and outgoing electronic traffic, email, context sensitive search on key words):		
Received By (name, title, organization, Center or Agency):		
Signature:	TCED case number	Date:

WARNING: This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) or other applicable laws or restricted from disclosure based on NASA policy. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).

Receipt of Targeted Collection of Electronic Data Records

Date:	Requestor Case or Activity Number: TCED case number
Provider of Records (name, title, organization, Center):	
Description of Records (media type, quantity, format, content):	
Received all necessary records for this case. <input type="checkbox"/> Yes <input type="checkbox"/> No	Comments:
Received By (name, title, organization, Center or Agency):	
Signature:	Date:

WARNING: This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) or other applicable laws or restricted from disclosure based on NASA policy. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).