



NASA Standard Operating Procedure

Procedures for Initiating and Managing Targeted Monitoring of Electronic Data

ITS-SOP-0008

Version: 20060303

Effective Date: March 3, 2006

Expiration Date: March 3, 2008

Responsible Office: Chief Information Officer

Procedures for Initiating and Managing Targeted Monitoring of Electronic Data

Introduction

This Standard Operating Procedure (SOP) establishes the procedures for initiating, managing and terminating targeted monitoring of electronic data on NASA networks and systems, when necessary to investigate suspected instances of inappropriate, illegal, or intended harmful use of NASA IT and information resources. Its purpose is to ensure that targeted monitoring is performed fairly and consistently across the Agency in a manner that prevents misuse of targeted monitoring; ensures due diligence when requesting, approving, and performing targeted monitoring; and promotes a productive work environment at NASA.

The procedures in this SOP apply to targeted monitoring of all NASA Internet Protocol (IP) space, wired and wireless networks, local area networks, wide area networks, virtual private networks, remote access to NASA networks, and external traffic traveling to and from NASA networks. They also apply to information stored on NASA computer systems, such as logs and the contents of hard drives and other electronic storage media. Telecommunications data such as telephone communications, telephone records and Voice over IP (VoIP) transmissions are not covered by this SOP.

Monitoring refers to the capture, review, and inspection of electronic data while in transit or in storage. Routine monitoring is general capture, review and inspection of electronic data for the purposes of providing effective IT services, protecting NASA networks and systems, and ensuring compliance with NASA policies. Targeted monitoring is specific or prolonged monitoring, based on an individualized suspicion or other justification, of electronic data that is linked to particular individuals or entities. As defined in NPR 2810.1, targeted monitoring can be initiated for the following reasons:

- A higher than expected volume of network traffic is detected on an individual's system;
- Hostile, threatening, suspicious, or unusual network traffic is detected;
- Connections to known hostile or precarious sites are identified;
- Unauthorized services or software are detected;
- A violation of NASA policy is detected;
- By approved request from Center monitoring staff, the Office of the Inspector General (OIG), the Office of Security and Program Protection (OSPP), a Center Office of Human Resources (OHR), the Office of Human Capital Management (OHCM), a Center Office of the Chief Counsel (OCC), or the Office of the General Counsel (OGC); or
- By court order.

NASA computers and networks are property of the U.S. Government. As stated in NPR 2810.1 and in the warning notice that appears on NASA computers, any NASA

employee or other user of NASA information systems shall have no expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of NASA computers and networks.

Targeted Monitoring

Targeted monitoring for IT security, law-enforcement, or administrative purposes may result from a variety of circumstances including the following:

- **Data found during routine monitoring:** During the course of routine network monitoring performed as part of their regular duties, monitoring staff may detect anomalous or suspicious network traffic that may warrant further inquiry and monitoring. This information is passed to the Center IT Security Manager (ITSM) or NASA IT Security Officer (ITSO) (see Appendix B), via the established procedures and reporting chain. The Center ITSM or NASA ITSO reviews the information and proceeds according to incident handling and response procedures established in NPR 2810.1 and other NASA IT security policies. The Center ITSM or NASA ITSO may determine that targeted monitoring is warranted without, prior to, or in addition to, law enforcement involvement. In this case, targeted monitoring may be formally requested by the monitoring staff or Center ITSM, approved by the Center Chief Information Officer (CIO), Center ITSM or NASA ITSO and performed under the same authority as routine monitoring. Monitoring results are delivered to the Center ITSM or NASA ITSO.
- **A management request:** A NASA civil service supervisor may have a need for monitoring of a civil service employee's use of NASA computer equipment or resources for the purpose of investigating suspected misuse (as defined in NPD 2540.1F, Personal Use of Government Office Equipment Including Information Technology, and in NPR 2810.1). Such a request is reviewed by the Center's Human Resources Employee Relations Specialist (see Appendix B), in consultation with OGC or the Center OCC if applicable. Targeted monitoring may then be formally requested by the Center OHR and approved by the Center CIO, Center ITSM or NASA ITSO. Contractor managers or NASA tenants may also have a need for monitoring their employees' use of NASA computer equipment or resources, requiring assistance from Center or NASA monitoring staff. Such monitoring will be reviewed and formally requested by OGC or the Center OCC and approved by the Center CIO, Center ITSM or NASA ITSO, as applicable. Monitoring is performed under the authority of and in support of the requestor. The Center ITSM delivers the requested monitoring results to the official requestor for distribution to the original management official as appropriate.
- **An OIG request:** During the course of a criminal or administrative investigation, the OIG may formally request NASA to perform targeted monitoring of one or more computers, IP addresses, or individual users on behalf of the OIG. Depending on the scope of the requested monitoring, the Center CIO, the Center ITSM or the NASA ITSO approves the request. Monitoring is performed under the authority of and in support of the requestor. (Note: the OIG has an independent capability, both technical and legal, to conduct monitoring in support of criminal investigations. This SOP

applies only to instances where the OIG requests technical assistance in performing targeted monitoring, not to ordinary requests for information on NASA network topologies, assistance in identifying individuals by network addressing, and nominal routing of network traffic to accommodate OIG monitors.)

- **An OSPP request:** During the course of a counter-intelligence (CI) investigation or other OSPP investigation, OSPP may formally request NASA to perform targeted monitoring of one or more computers, IP addresses, or individual users on behalf of OSPP. Depending on the scope of the requested monitoring, the Center CIO, the Center ITSM or the NASA ITSO approves the request. Monitoring is performed under the authority of and in support of the requestor.
- **An external law enforcement request or other external request:** External requests for monitoring of NASA computers, IP addresses or individual users will be routed through OSPP if the request has CI implications or through the OIG if there are other law enforcement implications.

Targeted monitoring may be approved by a Center CIO or Center ITSM for Center-specific monitoring or for monitoring related to Agency-wide IT resources hosted or managed at the Center. When multiple Centers are involved, it may be necessary for the requestor to coordinate with multiple Centers and to have each Center approve a targeted monitoring request for that Center. If necessary, the NASA ITSO may approve requests for monitoring at multiple Centers or at the Agency level. When reviewing a request, the Center CIO, Center ITSM or NASA ITSO should make sure that the authority under which monitoring will be performed is clear and that the requestor has provided justification for targeted monitoring. No targeted monitoring activity may be requested and approved by the same person.

A monitoring request can apply to existing data, as available, such as saved logs, archived network traffic, or the contents of storage media. The end date of such a targeted monitoring activity shall be no later than three months from the start date. A monitoring request can also refer to capture and inspection of new data, monitored for up to three months. After three months, a review and resubmission of each request are required to extend targeted monitoring for another three months. At the conclusion of the monitoring activity, the Center ITSM/NASA ITSO and/or monitoring personnel will require a receipt acknowledging that official monitoring results were provided to the requestor.

All requests for targeted monitoring must be completed by the official requestor as follows:

Request resulting from ...	Official Requestor
Data found during routine monitoring management request	monitoring staff or Center ITSM OHR or OGC/OCC
OIG investigation	OIG
OSPP investigation	OSPP
external law enforcement/other external request	OIG or OSPP

Monitoring requests should include as much detail as possible (without compromising an investigation or disclosing sensitive information) so that the targeted monitoring activity can be effective and sufficiently focused. Monitoring requests should contain specific requirements for targeted monitoring (e.g., monitoring all incoming and outgoing activity to/from particular IP addresses; monitoring traffic on particular ports; monitoring for specific information) and for data storage and handling.

Before approving targeted monitoring for law-enforcement purposes, the Center CIO, Center ITSM or NASA ITSO must receive an official case number from the requestor.

If an official case number is not required or not available for the targeted monitoring activity, i.e. if the request is not for law-enforcement purposes, the Center CIO, Center ITSM or NASA ITSO should assign a sequential identifier (or activity number) for tracking. This number should include the relevant Center and the date of the request (e.g. ARC-09152005-01). Such a number is helpful for matching data receipts to a particular monitoring activity and for general tracking if there is no official case number.

Procedures

When targeted monitoring is necessary, the following procedures will be followed:

(NOTE: These procedures refer only to initiating, managing and completing actual targeted monitoring, once an official requestor has determined that targeted monitoring is needed. The procedures do not include any initial review by OHR or other preliminary evaluation of whether monitoring should occur.)

1. The official requestor fills out and signs the form *Request for Targeted Monitoring* from Appendix A of this SOP.
2. The Center CIO, Center ITSM or NASA ITSO signs the request form after reviewing it to ensure that all required information was completed and that the request is appropriate and feasible.
3. The Center ITSM or NASA ITSO presents the approved request to the relevant monitoring staff and instructs them to proceed. The Center ITSM/NASA ITSO and monitoring staff, in consultation with the requestor, agree on how monitoring should occur, including
 - a. When and how often monitoring staff will report results and to whom;
 - b. What kind of data, if found, will be collected and delivered;
 - c. Media, format and delivery method for monitoring results;
 - d. How long monitoring staff will retain monitoring results after they have been delivered to the requestor (if applicable, to assist the requestor).
4. If applicable, the requestor briefs monitoring staff on data handling and storage requirements. Monitoring staff may be asked to sign a non-disclosure agreement.
5. The Center ITSM retains the approved request form on file. For Agency-wide or multi-Center targeted monitoring activities, the NASA ITSO retains a copy.

Monitoring request forms shall be transmitted only via NASA-standard encrypted email, fax, mail, or hand delivery.

6. Targeted monitoring is performed as approved.
7. Once monitoring is completed or as agreed between the requestor, the Center ITSM/NASA ITSO and the monitoring staff, results from the targeted monitoring are turned over to the requestor or an additional point of contact (POC) specified in the request form. Upon receipt of the material, the requestor signs a receipt acknowledging that the monitoring was conducted and that he or she received the requested materials. The form *Receipt of Targeted Monitoring Records* in Appendix A of this SOP is used. Because data may be provided to the requestor on multiple occasions during the course of a targeted monitoring activity, multiple receipts may be necessary. All receipts are maintained in the Center ITSM's files.

As stated in NPR 2810.1, the Center ITSM will notify law enforcement of any new suspected criminal activities identified during targeted monitoring.

Termination of Targeted Monitoring

At the end of a targeted monitoring request, or sooner if instructed by the requestor or the Center ITSM/NASA ITSO, the monitoring staff will cease targeted monitoring.

All results will be provided as agreed via the Center ITSM or NASA ITSO to the requestor or additional POC specified on the request form. The requestor will sign a receipt acknowledging that the monitoring was completed and that he or she received the requested materials. It is up to the requestor to verify that complete results in a readable format were received. If necessary the Center ITSM or monitoring staff should provide technical assistance. Once all requested data has been provided to the requestor, this data becomes the sole responsibility of the requestor.

After monitoring results have been provided to the requestor, the monitoring staff has no further requirement under this SOP to retain the results. However, they may retain copies, for example to assist the requestor as previously agreed, as advised by the Center ITSM/NASA ITSO, or to conform to Center retention policies. When deleting monitoring results data, this will be done in accordance with NPR 1600.1 requirements for SBU information.

Data Handling and Storage

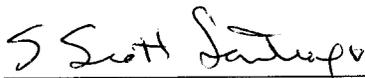
When targeted monitoring is related to a criminal or CI investigation, specific procedures for handling and storing monitoring results may be necessary to preserve legal evidence or to protect sensitive or confidential information. If such requirements exist, the requestor should be prepared to brief the monitoring staff and to provide additional training and assistance as needed.

Monitoring staff are expected to follow, within reason, any specific data handling and storage procedures as instructed by the requestor. In addition, monitoring staff are

expected to keep confidential all details of any targeted monitoring activities and may be asked to sign a non-disclosure agreement. Information related to targeted monitoring activities will be transmitted only using NASA-standard encryption, fax, mail or hand-delivery.

Recipients of targeted monitoring results (i.e. requestors or their delegates) are also expected to handle, store, and dispose of monitoring data in accordance with applicable NASA and Federal policies. This includes, for example, destroying data from a targeted monitoring activity which found no actionable activity.

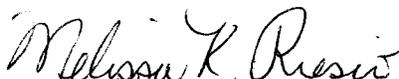
All requests for targeted monitoring will be retained by the Center ITSM, with copies sent to the NASA ITSO for multi-Center or Agency-wide requests. All receipts for results from targeted monitoring will be retained by the Center ITSM. Documentation of targeted monitoring activities may contain sensitive information and must be handled and stored in accordance with NPR 1600.1 requirements for Sensitive But Unclassified (SBU) information.



S. Scott Santiago
Deputy Chief Information Officer
for IT Security
Office of the Chief Information Officer

3/3/06
Date

Concurrences



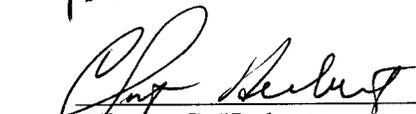
Melissa Riesco
Acting Director, Workforce
Management and Development Division
Office of Human Capital Management

3/21/06
Date



Robert W. Cobb
Inspector General *for*

17 Mar 06
Date



Clinton G. Herbert
Deputy Assistant Administrator
Office of Security and Program Protection

23 Mar 06
Date

Appendix A

Forms

Request for Targeted Monitoring

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

Date of Request:	Secure Data Exchange: <input type="checkbox"/> Entrust <input type="checkbox"/> PGP
Requestor (name, title, organization, Center):	Contact Information Phone: Fax: E-mail:
Signature:	Date:
Other Approved POC(s):	

Case/Activity Number:	Requested Start Date:
<input type="checkbox"/> Routine Monitoring Found Anomalous/Suspicious Activity <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 name(s) if applicable, system IP/domain information):	
Specific Monitoring and Storage/Handling Requirements (e.g., monitor all incoming and outgoing electronic traffic, email, context sensitive search on key words, etc.):	
Staff to Perform Monitoring:	

Start Date:	End Date (3 months or less):
Approving Center CIO/Center ITSM/NASA ITSO (name, Center, phone, email):	
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).

Receipt of Targeted Monitoring Records

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

Appendix B

Points of Contact

NASA Points of Contact for Targeted Monitoring of Electronic Data

The following information is current as of the dates stated.

Center IT Security Managers (as of 03/01/2006)

Center	POC	Phone	E-Mail Address
NASA ITSO	Michael Castagna	202-358-2325	michael.j.castagna@nasa.gov
ARC	Helen Stewart	650-604-4678	Helen.j.stewart@nasa.gov
DFRC	Larry Johnson	661-276-3869	larry.d.johnson@nasa.gov
GRC	Pam Kotlenz	216-433-5164	Pamela.Kotlenz@grc.nasa.gov
GSFC	Hank Middleton	301-286-2486	henry.j.middleton@nasa.gov
HQ	Greg Kerr	202-358-2218	gkerr@nasa.gov
JPL	Jay Brar	818-354-9632	Jatinder.S.Brar-100262@jpl.nasa.gov
JSC	Chris Ortiz	281-483-1904	Christopher.j.ortiz@nasa.gov
KSC	Glenn Seaton	321-867-9065	glenn.seaton@nasa.gov
LaRC	Kendall Freeman	757-864-6670	kendall.e.freeman@nasa.gov
MSFC	David Black	256-544-5942	david.g.black@nasa.gov
NSSC	James Cluff	228-688-2249	James.Cluff@ssc.nasa.gov
SSC	Christine Reynolds	228-688-3919	Christine.L.Reynolds@nasa.gov

Center Human Resources Employee Relations Specialists (as of 06/14/2005)

Center	POC	Phone	Email Address
ARC	Mike McCartney	650-604-2896	Michael.F.McCartney@nasa.gov
DFRC	Connie Bosworth	661-276-2397	connie.s.bosworth@nasa.gov
GRC	Lori Pietravoia (ER/LR)	216-433-2506	Lori.O.Pietravoia@nasa.gov
GSFC	Tina LaFountain (ER)	301-286-3729	Christina.Lafountain-1@nasa.gov
HQ (Operations)	Dorothy Egbert	202-358-1162	dorothy.s.egbert@nasa.gov
HW (OIG)	Omar Williams	202-358-2137	omar.d.williams@nasa.gov
JSC	Vanessa Bowen	281-483-3084	vanessa.bowen-1@nasa.gov
KSC	Frank Nesbit (ER)	321-867-7293	Frank.L.Nesbit@nasa.gov
	Jim Thompson (LR)	321-867-7484	James.V.Thompson@nasa.gov
LaRC	Nancy Davis (ER)	757-864-2686	Nancy.T.Davis@nasa.gov
MSFC	Mack Blackman (ER)	256-544-7509	William.M.Blackman@nasa.gov
	Kevin Plank (LR)	256-961-0157	Kevin.Plank@nasa.gov
SSC	Dorsie Jones (ER)	228-688-2337	Dorsie.Jones-1@nasa.gov

Office of General Counsel POC for Targeted Monitoring Questions (as of 01/19/2006)

David Barrett
 Office of the General Counsel
 202-358-2027
 david.g.barrett@nasa.gov