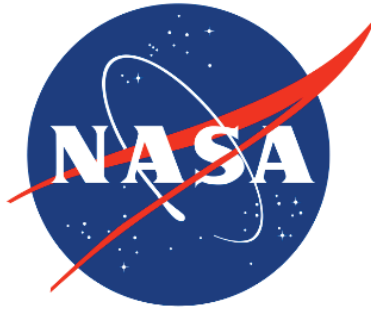




Information Technology Security Handbook

Collection of Electronic Data

November 2023

Version 3.0

OFFICE OF THE CHIEF INFORMATION OFFICER

CYBER SECURITY AND PRIVACY DIVISION

Document Properties

Maintained by: OCIO CSPD Team

Filename: ITS-HBK-2810.09-03B Collection of Electronic Data

Supersedes:

Version 2.1

Table 1: Revision History

Version	Date	Change Description
1.0	8/10/2018	Handbook updated and separated from the Incident Response handbooks that are being consolidated and revised by the NASA SOC. Replaces the “Targeted Collection of Electronic Data” handbook and addresses attempt to change name of activity to “Focused Cyber Analysis.”
1.0	7/30/2019	SAISO approved and signed the updated handbook.
2.0	6/30/2020	To simplify the CED process, CSPD in collaboration with NASA stakeholders developed a NASA Standard Electronic CED Form NF1853. NF1853 has all the required information fields and digital signature fields.
2.1	9/29/2020	Minor grammatical edits. Added SBU marking.
3.0	11/3/2023	Reviewed and updated to align with OCIO transformation and clarifying the differences between this handbook and ITS-HBK-2810.09-04, Incident Response and Management: Guidelines for Data Spillage and Sanitization Procedures. Handbook also updated to reflect transition from PCAT to RISCS. Separation and clarification of sections for Privacy Act records. Other minor edits and updates. Reviewed by privacy personnel at the center and agency level. Removed SBU marking.

Table of Contents

1. INTRODUCTION	1
1.1 Purpose	1
1.2 Scope	2
1.3 Point of Contact(s)	3
1.4 Applicability	3
1.5. APPLICABLE DOCUMENTS	3
2. ROLES AND RESPONSIBILITIES	4
2.1 Agency-Wide	4
2.2 The FOIA Office	6
2.3 Center Level	6
2.4 Information System Level	6
3. OVERVIEW OF CED ACTIVITY REQUIREMENTS	7
4. CED PROCESS AND PROCEDURES	9
4.1 Initiating a CED Activity	9
4.2 Managing a CED Activity	10
4.3 Ending a CED Activity	11
4.4 Handling and Storing Data from a CED Activity	11
Appendix A: Collection of Electronic Data Forms	13
Appendix B: Acronyms	14
Appendix C: Request Types, Data Requested, Approval Required	16
Table 1: Revision History	iv
Table 2: Purposes/Types of CED Requests	8

This page intentionally left blank.

Distribution

NODIS



Associate Chief Information Officer
for Cybersecurity & Privacy

1. INTRODUCTION

The National Aeronautics and Space Administration (NASA) adheres to guidance from the National Institute of Standards and Technology (NIST) to protect information and information systems. Information System Owners (ISOs) and other personnel responsible shall categorize information and information systems according to NIST-defined security objectives (i.e., confidentiality, integrity, and availability). ISOs and other personnel shall determine an information systems baseline controls using NIST-defined criteria. NIST objectives and criteria are referenced in:

- Federal Information Processing Standards (FIPS) 199 publication, Standards for Security Categorization for Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations is the basis for selecting security and privacy controls, resulting from categorizing an information system and the information it collects, stores, processes, and/or transmits. The NIST Risk Management Framework defines the process used to manage risk across the life cycle (See NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy).

NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information and Information Systems, and the collection of 2810 Information Technology Security handbooks (ITS-HBKs) satisfy the policy and procedure controls of NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

This handbook supports implementation and verification compliance with requirements in NPR 2810.1, NPD 2810.1, and NPD 2540.1, Acceptable Use of Government Furnished Information Technology, Equipment and Services . It also augments NIST guidance with NASA-specific requirements, procedures, and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organization-defined values are integrated into control requirements in the Risk Information Security Compliance System (RISCS) system.

1.1 Purpose

This handbook establishes the processes and procedures for initiating, managing, and ending the collection and analysis of NASA electronic data. The Collection of Electronic Data (CED) is defined as the "collection and analysis of data in an electronic form to provide information about a NASA user's use of NASA information system resources." Former names for CED include "Targeted Collection of Electronic Data" and "Focused Cyber Analysis." CED is a

distinct process from those described in ITS-HBK-2810.09-04, Guidelines for Data Spillage and Sanitization Process. Personnel addressing spillage and sanitization need to reference ITS-HBK-2810.09-04.

This handbook also provides information about 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
- Counterintelligence (CI) investigation
- A response to business continuity requirements

The requirements set forth in this handbook help to:

- Ensure that the utilization and application of a CED is fair, reasonable, and consistent throughout NASA
- Prevent the abuse or misuse of a CED
- Ensure enough justification exists to initiate a CED
- Ensure due diligence when requesting and performing a CED
- Terminate the CED within mandated time constraints

1.2 Scope

The processes and procedures in this handbook apply to all requests to initiate collection and conduct analysis of data about a NASA user's use of NASA information system resources.

The SOC and Cybersecurity Incident Response Team (CIRT) manage the potential for and actual damage and disruption to information systems. An incident is any violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident may result in or stem from any one of the following: a failure of security controls, an attempted or actual compromise of information, and/or waste, fraud, abuse, loss, or damage of government property or information.

CEDs may be initiated and are limited to support:

- Administrative or criminal investigations as outlined in *NPR 2810.1F*, or otherwise required by law.¹
- CI investigations, when requested by the Office of Protective Services (OPS).
- Collecting information needed for business continuity such as the departure of a NASA employee for any reason without proper coordination (e.g.,

¹ Not necessarily an investigation of the target user, but possibly an investigation into a security breach that affected information resources the user produces, owns, and/or interacts with.

- change of role, resignation, retirement, dismissal, or death).
- Recovery of electronic information from “damaged” devices, such as hard drive recovery.

Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to NPR 1400.1, portions of NASA handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

This handbook and the procedural guidance contained within remains in full force and effect until such time that the handbook is formally cancelled, rescinded or superseded by an updated document.

A documented rationale/justification will accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this handbook to support such a decision. The documented rationale/justification will be provided to the NASA Cybersecurity and Privacy Division (CSPD), in coordination with the Center Chief Information Security Officers (CISOs), to review and validate.

1.3 Point of Contact(s)

For any questions or comments regarding the contents of this handbook, contact:

- hq-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation will be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular handbook to address and resolve.

1.4 Applicability

This handbook applies to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

1.5. APPLICABLE DOCUMENTS

- ***National Aeronautics and Space Administration***
 - NPD 2540.1, Acceptable Use of Government Furnished Information Technology, Services and Resources.

- NPR 1441.1, NASA Records Management Program Requirements (Updated w/Change 3)
 - NPR 1600.1, NASA Security Program Procedural Requirements.
 - NPR 1600.2, NASA Classified National Security Information (CNSI.)
 - NPR 2810.1, Security of Information and Information Systems.
 - ITS-HBK-2810.09-02, Incident Response and Management: NASA Information Security Incident Management.
- ***Cancellations or Updates***
- ITS-HBK-2810.09-03A, Incident Response and Management: Collection of Electronic Data, June 1, 2020

2. ROLES AND RESPONSIBILITIES

2.1 Agency-Wide

- *The NASA Chief Information Officer (CIO):*
- Informs NASA Senior Management of a CED, as appropriate.
 - Delegates to the Senior Agency Information Security Officer (SAISO) the responsibility and accountability for the NASA-wide implementation of the NASA CED handbook processes.
- *The Senior Agency Information Security Officer (SAISO):*
- Maintains responsibility and accountability for the NASA-wide implementation of NASA CED policies and processes.
 - Informs the NASA CIO about CED activities and findings, as appropriate.
 - Reviews and approves or disapproves the CED investigation-related requests following review of request by the NASA Office of General Counsel (OGC).
 - Delegates authority to approve and/or process CED requests, as deemed appropriate, depending upon the source or justification for the request.
- *The NASA Security Operations Center (SOC) Operations Manager:*
- Informs the SAISO about CED activities and findings, as appropriate.
 - After approval is received from vetting authorities, reviews and assigns resources for CED requests from authorized NASA managers and law enforcement officials.
 - Maintains visibility of all CEDs through ticketing in the SOC Incident Management System (IMS).
 - Utilizes all resources and personnel, as appropriate, to fulfill the CED within the scope of data and access.
 - Maintains documentation of all CED activities, including law enforcement or other requests for a CED and receipts for CED records.
 - Assigns case numbers to all CED requests.
 - Ensures that all CED requests, regardless of source or justification, are tracked/monitored and documented.

- Involves CISOs and CIRT to assist in the CED as appropriate and necessary.
- *The NASA Contracting Officer:*
 - Initiates request to the OGC, if necessary, to investigate a contract employee's use of NASA computer equipment or resources for suspected misuse.²
 - Engages the Contracting Officer Representative (COR), as appropriate.
 - Reports closure of all CED when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
- *The Office of the Inspector General (OIG):*
 - Reviews and validates all requests for a CED from the OIG to ensure they comply with the procedural requirements of this handbook.
 - Submits properly vetted requests to the SAISO, ISO, or SOC when requesting support for a CED.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
 - Establishes and maintains direct access to the eDiscovery capability in Office 365 for NASA OIG criminal investigations, subject to oversight, auditing and/or monitoring by the NASA SOC of the OIG eDiscovery access process.
- *The Deputy Assistant Administrator for the Office of Protective Services (OPS):*
 - Reviews and validates all requests for a CED from OPS to ensure they comply with the procedural requirements of this handbook.
 - Formally requests NASA to perform a CED during a CI investigation or other OPS investigation.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
- *The Office of the General Counsel (OGC):*
 - Reviews all CED requests for legal sufficiency prior to SAISO review and approval.
 - Reviews CED requests from contractor managers and formally requests CEDs on their behalf, if appropriate.
 - Upon request from the Office of the Chief Human Capital Officer (OCHCO) assists OGC to determine whether to make a formal request for a CED.
 - Submits requests for the initiation of a CED in support of court orders or other legal actions.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
 - Concurs with the FOIA office to initiate collections pursuant to Freedom of Information Act requests without prior OGC review.

² The OGC will then submit a formal CED initiation request on the Contracting Officer's behalf, as appropriate.

2.2 The FOIA Office

- *The FOIA office will be responsible for requesting and directing collections and searches pursuant to Freedom of Information Act requests. These requests have been pre-approved by the Agency CIO, the SAISO, and OGC.*

2.3 Center Level

- *The Center CIO:*
 - Informs the Center Director of CED activity and findings, as appropriate.
 - Maintains a technical capability to support a reasonable number of CED requests.
 - Negotiates with requesting parties when resource constraints are identified in supporting a CED.
- *The Center Human Resource Office Specialist of the Office of Chief Human Capital Officer:*
 - Reviews requests from supervisors for a CED and requests help from the OGC in evaluating those requests.
 - Coordinates CED request with SOC.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
- *The NASA Civil Service Supervisor:*
 - Submits CED initiation requests to the Center's Human Resources Office Specialist in consultation with the OGC, if applicable, to monitor a civil service employee's use of NASA computer equipment or resources for suspected misuse.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
- *The Contractor Supervisor:*
 - Submits CED initiation requests to the CO: *The CO, in consultation with OGC, determines appropriate action based on the request (see provision above).*
- *The Office of the General Counsel (OGC):*
 - Reviews CED requests for legal sufficiency prior to SAISO review and preliminary approval.
 - Submits requests for the initiation of a CED in support of court orders or other legal actions affecting Centers.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.

2.4 Information System Level

- *The Information System Owner (ISO):*
 - Receives requests for initiation of a CED.

- Supports properly vetted CED requests.
 - Notifies the SAISO or SOC of CED requests, as appropriate.
 - Obtains a CED case number from the NASA SOC.
 - Arranges for resources capable of supporting a CED.
 - Informs SAISO, CISO, or NASA managers regarding the results of the CEDs, as appropriate.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
- *Individual or IT Service Provider supporting a CED:*
 - Ensures that all requests for a CED are properly documented and archived in coordination with NASA SOC tools, policies, and processes.
 - Provides technical support and monitoring services for an authorized CED.
 - Informs the SAISO, CISO, or ISO on the progress and results of a CED, as appropriate.
 - Ensures the CED is closed when the monitoring and/or collection period ends and the results of the CED are delivered to the requestor of the CED.
 - Properly safeguards all data collected while conducting a CED.
 - *The NASA User:*
 - Reports actual or suspected misuse of IT resources to the NASA SOC, Center CISO, or other appropriate officials.

3. OVERVIEW OF CED ACTIVITY REQUIREMENTS

This section establishes procedures and/or justifications for requesting, initiating, conducting, and terminating a CED. All CED activities must follow the processes set forth in this handbook. No CED may be initiated or conducted without proper vetting and approval as set forth in this handbook. Except for CEDs initiated by OIG investigations, all CEDs must be reviewed for legal sufficiency, adequate justification under this handbook, and approved by the SAISO or designee.

All CED activities are divided into three phases:

1. Requesting/initiating a CED activity – submission of a signed *Request for Collection of Electronic Data form*
2. Managing a CED activity – develop and oversee a CED management plan
3. Ending a CED activity – deliver results of the CED activity and closing out the action

Initiate and conduct a CED only under the appropriate legal authority and NASA policy requirements. The governance framework for a CED should be carefully considered to ensure limiting exposure of the data collected through separation of duties and need-to-know practices. The person or organization who requests a CED may not validate/approve the same CED.

A CED may be initiated for any of the following lawful justifications:

- Actual or suspected inappropriate, illegal, criminal, or intentional harmful use of NASA information systems and resources
- CI investigation
- An actual or suspected violation of NASA policy governing Information Technology or Information Security
- A valid and enforceable order from a court or other administrative body
- A statutory or regulatory requirement (e.g., Freedom of Information Act requests, investigatory requests from the Office of Special Counsel)
- Pending or anticipated litigation as identified by the Office of General Counsel or pursuant to the procedures in *NASA Procedural Requirement 1441.1*, Chapter 4
- Business continuity requirements (such as when an employee leaves their position at NASA without proper coordination for any reason or on extended medical leave)

Table 2: Purposes/Types of CED Requests

Type of Request	Description	Use-cases/examples	Notes
Business Continuity	Required for continuity of operations.	1. A person is on an extended absence from work and is unable to provide the data. 2. A person is terminated. 3. A person passes away.	
Non-criminal employee or affiliate activity	NASA employee or affiliate non-criminal investigation or suspected activity that requires the collection of data.	1. Suspected misuse of government IT equipment and/or resources. 2. Violations of acceptable use policy.	
Criminal employee or affiliate investigation	Collection of data to support a criminal investigation		Can only be initiated by OIG.
Counterintelligence			Can only be initiated by CI.
FOIA			Can only be initiated by FOIA Office

The following may receive a request for a CED and initiate a CED depending upon the intended purpose or justification of the CED:

- OIG
- OGC³
- Deputy Assistant Administrator, OPS, for CI investigations

³ Not necessarily an investigation of the target user, but possibly an investigation into a security breach that affected information resources the user produces, owns, and/or interacts with.

- Center Human Resources Employee Relations Specialist (Office of Human Resources or OHCM)
- Others, such as the Center CISO, ISO, ISSO

A CED request may apply to:

- Available existing data, such as saved logs, archived network traffic, email, or the contents of storage media
- Collection and data analysis not previously collected

The individual supporting the CED shall consider all data related to the CED as sensitive information (i.e., Controlled Unclassified Information (CUI) or classified national security information) regardless of classification of the CED, and will apply all protections required for sensitive or classified national security information while handling and storing this data. Additional handling requirements may be imposed by the requestor due to heightened sensitivity or classification of the data. The individual supporting the CED shall follow, within reason, any specific data handling and storage procedures that the requestor requires.

4. CED PROCESS AND PROCEDURES

4.1 Initiating a CED Activity

Once a CED request is initiated or created, the requestor should monitor activity to ensure the CED request is properly managed through every stage of the process by others involved in this process to include the recipient of the CED request and the individual supporting the request. The requestor should track the progress of the CED request from initiation to closure.

To initiate a CED request, a requestor must complete and submit NASA Electronic Form NF 1853 "Request for/ Receipt of Collection of Electronic Data" (Appendix A) to the recipient as appropriate for the CED. NF 1853 is available at the NASA Electronic Forms website (<https://nef.nasa.gov/nef/search?query=1853¢er=10¢er=1>). Requestors shall obtain a CED case number from the NASA SOC to assure consistent tracking. In addition, all CED tracking and CED number assignments will use the SOC's Incident Management System (IMS). The SOC will provide the IMS case number to all parties involved in the CED activity.

CED requests should 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 requests shall specify the collection, monitoring, review, and analysis requirements (for example, user identification, all incoming and outgoing activity to or from a given IP address, all traffic on specified ports, or all traffic about specified information), that include:

- Any special requirements for data storage and handling
- Parties to be notified
- Methods of communicating results

The recipient of the CED request shall identify any resource constraints and work with the requestor to build an acceptable management plan. The management plan should be attached to the Request for Collection of Electronic Data form when submitted for legal review and approval.

Upon receipt of the completed CED form, the recipient will ensure:

- The Request for/ Receipt of NF 1853 Collection of Electronic Data form (Appendix A) is completed in full.
- That they and the requestor create an acceptable management plan for the CED and attach it to the Request for Collection of Electronic Data form.
- The SOC has assigned a case number for the CED and that case number is reflected on the Request for Collection of Electronic Data form.
- The authority and/or justification under which the proposed monitoring will take place is unambiguous (and meets the legal reasons for conducting a CED listed in this handbook).
- The organization can support the requested CED action.
- The appropriate management roles are clear and have been made aware of the CED.
- The appropriate level legal office has reviewed and/or vetted the CED request.
- The resources and needed data sources to support the CED request have been identified.

4.2 Managing a CED Activity

The recipient of the CED request will implement a CED management plan that includes:

- When and how often the individual supporting the CED reports results and to whom.
- What kind of data, if found, is collected and delivered.
- The media, format, and delivery method for the CED results.
- How long the individual supporting the CED will retain the results after delivering them to the requestor, if applicable.

The individual(s) supporting the CED will carry out the collection, monitoring, review, and analysis as agreed and authorized. The results shall be submitted to the recipient of the CED request for review upon completion of the CED and before delivery to the requestor. If the ISO is the recipient of the CED request, the ISO will communicate the completion of the CED to the SAISO and/or CISO as appropriate.

It is the requestor's responsibility to verify that complete results were received in a readable format. If necessary, the requestor of the CED may ask for technical assistance from the recipient of a CED or the individual supporting the CED.

4.3 Ending a CED Activity

The monitoring and/or collection period terminates upon expiration of the approved/authorized period, not to exceed six months. The individual supporting the CED notifies both the recipient of the CED request and the requestor of the CED request when the collection period for the CED request ends and confirms that the monitoring and/or collection is complete.

When the monitoring and/or collection period ends the results shall be delivered to the requestor of the CED. The end date of a CED shall not exceed six months after the start date for the CED.

Upon receipt of the results, the requestor will sign the receipt form, Request for/Receipt of Collection of Electronic Data Records (Appendix A), acknowledging that monitoring/collection results were received and that the CED is complete. By doing so, the requestor of the CED accepts responsibility for the information and ensures that the CED activity is promptly closed.

4.4 Handling and Storing Data from a CED Activity

The individual supporting the CED shall follow, within reason, any specific data-handling and storage procedures that the requestor requires. The individual supporting the CED will also keep all details of any CED confidential, and they may be required to sign a non-disclosure agreement (NDA). Any information that results from or is related to a CED shall only be transmitted using NASA-standard encryption, fax, mail, or hand-delivery.

The individual supporting the CED 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, CISO, or ISO. When the individual supporting the CED deletes the results, they shall follow the NPR 1600.1 requirements for destroying sensitive information.

The individual who receives the CED results (such as requestors of the CED or their designated points of contact) shall also handle, store, and dispose of monitoring or collection data in accordance with all applicable NASA and Federal policies. This includes, for example, destroying the data from a CED request that found no actionable or inappropriate activity.

When a CED is related to a criminal or counterintelligence investigation, it may be necessary to follow special procedures for handling and storing the monitoring/collection results to preserve legal evidence or to protect sensitive information. If such requirements exist, the requestor shall give the monitoring/collection staff any additional training and assistance

needed.

The SAISO and/or SOC shall also retain all receipts for the results of a CED delivered to the requestor for a minimum of three years. CED information may contain sensitive or classified information and should be handled, stored in accordance with NASA requirements for sensitive information (e.g., for CUI in accordance with NPR 2810.7) or classified information (NPR 1600.2).

Appendix A: Collection of Electronic Data Forms

As of the publication date of this handbook the image below belongs to NF 1853. However, you need to download the form at [NEF Search \(nasa.gov\)](https://www.nasa.gov/nef-search). Please read instructions carefully to ensure you are using the most updated version.

CUI when filled in



**Request for/ Receipt of Collection of
Electronic Data**

Definition and Scope

According to IT Security Handbook ITS-HBK-2810.09-03A, Collection of Electronic Data (CED), a CED 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." CED requests can be initiated to support:

- Administrative or criminal investigations as outlined in NPR 2810.1A (Security of Information Technology), NPR 1600.1A (NASA Security Program Procedural Requirements), and NPR 1600.3 (NASA Personnel Security Investigations), or otherwise required by law.
- Counter-Intelligence (CI) investigations, when requested by the Office of Protective Services (OPS).
- Collecting information needed for business continuity such as the departure of a NASA employee for any reason (e.g., change of role, resignation, retirement, dismissal, or death).
- Recovery of electronic information from "damaged" devices, such as hard drive recovery.

A CED request may apply to:

- Available existing data, such as saved logs, archived network traffic, or the contents of storage media, to include email.
- Collection and analysis of data not previously collected.

The end date of a CED shall not be later than six months after the start date.

Who can be a Valid Approver?
A valid approver for CED requests is based on the following case types:

Case Type	Valid Approver
Non-criminal NASA civil servant employee investigation	NASA HR Employee Relations team member, NASA Center Chief Counsel's Office, Chief Information Security Officer (CISO) or Office of General Counsel
Non-criminal NASA contractor employee investigation	Chief Information Security Officer (CISO), or Contracting Officer Representative (COR)
Business Continuity	Same as corresponding non-criminal [civil servant/contractor] employee case type
Criminal employee investigation	Office of Inspector General (OIG), Counter-Intelligence (CI), Protective Services (PS), Chief Information Security Officer (CISO), etc.
Freedom of Information Act (FOIA) request	FOIA Officer or Public Affairs (PX)
External organizational request	Chief Information Security Officer (CISO)

Instructions for Requestor

Complete all required requestor fields. Include as much detail as possible (without compromising an investigation or disclosing sensitive information) so that the activity can be sufficiently focused and effective. If the data is to be sent to a different point of contact other than the Requestor, specify in the "Data should be delivered to" field. When finished, sign the "Requestor signature" field and click the Submit button. Encrypt and send the auto-generated email to the Center specific first approver.

Center Chief Counsel review not required if requestor is OIG.

WARNING: This document is CONTROLLED UNCLASSIFIED INFORMATION (CUI). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), 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 CUI 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 official (see NID 2810.135).

NASA FORM 1853 10/22 (2.0) PREVIOUS VERSIONS ARE OBSOLETE. Validate prior to use.

Submit by Email

Page 1 of 3

Appendix B: Acronyms

CED	Collection of Electronic Data
CI	Counterintelligence Investigation
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CIRT	Cybersecurity Incident Response Team
COR	Contracting Officer's Representative
EP	Elevated Privilege(s)
FFRDC	Federally Funded Research and Development
FIPS	Federal Information Processing Standards
HBK	handbook
IMS	Incident Management System
IR	Incident Response
IRM	Incident Response Manager
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulation
ITS	Information Technology Security
NASA	National Aeronautics and Space Administration
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCC	Office of Center Chief Counsel
OCIO	Office of the Chief Information Officer
OCHCO	Office of the Chief Human Capital Officer
OGC	Office of General Counsel
OHCM	Office of Human Capital Management

OHR	Office of Human Resources
OIG	Office of the Inspector General
OPS	Office of Protective Services
OS	Operating System
PII	Personally identifiable Information
PGP	Pretty Good Privacy
POC	Point of Contact
RISCS	Risk Information Security Compliance System
SAISO	Senior Agency Information Security Officer
SBU	Sensitive But Unclassified
SOC	Security Operations Center
SP	Special Publication
VoIP	Voice over Internet Protocol

Appendix C: Request Types, Data Requested, Approval Required

Type of Request	Data Requested and Source	Approval Required	Team to action request
Business Continuity	Files: Druva backups Files: OneDrive Files: Physical Device Email: Office 365 User workstation	OGC	WCS or NASA SOC NASA CIRT
Non-criminal employee or affiliate activity	Files: Druva backups Files: OneDrive Files: Physical Device Email: Office 365 User workstation	OGC	NASA CIRT
Criminal employee or affiliate investigation	Files: Druva backups Files: OneDrive Files: Physical Device Email: Office 365 Forensic image of user workstation	OIG only	NASA SOC or NASA CIRT NASA CIRT
Counterintelligence	As specified by CI	CI only	As specified by CI
FOIA	Email: Office 365	OGC	WCS or NASA SOC