NASA Interim Directive

NID 2810.142
NPR 2810.2
Effective Date: December 5, 2023
Expiration Date: December 5, 2024

Subject: Possession and Use of NASA Information and Information Systems Outside of the United States

Responsible Office: Office of the Chief Information Officer (OCIO)

Preface

P.1 Purpose

a. This NASA Interim Directive (NID) document establishes requirements and responsibilities for the access, operation, and handling of NASA information, information technology, and networks by NASA Users outside of the United States.

b. Within this NID, the term United States includes the United States, the District of Columbia, and the commonwealths, territories, and possessions of the United States. In this directive the term international travel means travel outside the United States as in this paragraph.

P.2 Applicability

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

b. In this NID, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission; "should" denotes a good practice and is recommended but not required; "will" denotes expected outcome; and "are/is" denotes descriptive material.

c. This NID covers all devices that store, process, transmit, or receive NASA information including, but not limited to, contractor-provided or partner-provider devices as well as NASA-issued IT devices, such as laptops, tablets, Universal Serial Bus (USB) storage devices, cell phones, and smartphones when such devices are used or carried while outside the U.S.

d. This NID covers all non-public NASA information regardless of format and medium of storage, transport, and use. The use of unauthorized devices to access non-public NASA information for the conduct of official NASA business, including while outside the U.S., is not

allowed. This NID also covers downloads of information and information created during international travel.

e. NASA OCIO does not assess the purpose or value of international travel when enforcing the requirements of this NID. To the greatest extent possible, the OCIO shall support operations outside the U.S. as authorized by Agency policy and procedures.

f. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

P.3 Authority

a. Export Administration Regulations (EAR), 15 Code of Federal Regulations (CFR) pts. 730-774.

b. International Traffic in Arms Regulations (ITAR), 22 CFR pts. 120-130.

c. Federal Travel Regulations (FTR), 41 CFR pts. 300-304.

d. Federal Information Security Modernization Act (FISMA) 2014, 44 U.S.C. pt. 3551 et seq

e. NPR 2190.1, NASA Export Control Program.

f. NPR 2810.1, Security of Information and Information Systems.

g. NPR 9710.1, General Travel Requirements.

h. NASA Advisory Implementing Instruction (NAII) 2190.1, NASA Export Control Program Operations Manual.

i. Office of International and Interagency Relations (OIIR) Memorandum: Update on Training Requirements for NASA Official International Travel, November 28, 2018.

P.4 Applicable Documents and Forms

a. NPR 1382.1, NASA Privacy Procedural Requirements.

b. NASA Policy Directive (NPD) 2200.1 Management of NASA Scientific and Technical Information.

c. NPD 2540.1 Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources.

d. ITS-HBK-AASTEP0 through AASTEP6, NASA A&A Policy Handbooks (7 total)

e. ITS-HBK-2810.07-02, Configuration Management.

f. ITS-HBK-2810.11-02, Media Protection and Sanitization.

g. Designated Countries List: http://oiir.hq.nasa.gov/nasaecp/index.html (under Related Links)

h. NASA-SPEC-2675, International Travel

P.5 Measurement/Verification

Performance measures relative to implementation policy will be part of NASA's FISMA reporting and verification will occur through the NASA OCIO internal controls program.

Chapter 1. Requirements

1.1 Introduction

a. NASA information, information technology (IT), and networks must be protected. This NID outlines requirements and responsibilities to protect NASA information, IT systems, and networks while NASA personnel are outside of the U.S.

b. IT devices and systems are vulnerable to eavesdropping, interception, and theft. Operating outside the U.S. increases these risks, mainly where telecommunication networks are owned or controlled by the host government. IT devices are always at risk for introducing malicious software, and such risks are greater when devices leave the user's physical control. These risks are the greatest when traveling to or from The Russian Federation (hereafter referred to as Russia) or countries on the Designated Countries List (DCL) identified above in P.4g.

c. External directives and processes manage travel approval, concurrence, and authorization from non-OCIO entities, i.e., Office or International and Interagency Relations (OIIR) NPR 2910.1 compliance, Office of Protective Services (OPS), Office of Procurement (OP), Office of Chief Human Capital Officer (OCHCO), etc.

d. The OCIO shall confirm certain conditions are met before fulfilling the request for IT support for operations outside the U.S. When travel will be to or from Russia or a country on the DCL, this support will take the form of specially configured OCIO Workplace and Collaboration Services (WCS)-managed loaner devices and not the devices NASA Users use regularly while inside the U.S., per NASA-SPEC-2675. No other loaner devices or devices NASA Users use regularly shall be used for travel outside the U.S to or from one of these countries.

1.2 Use of NASA Information while Outside the U.S.

a. NASA Users shall take outside the U.S. only NASA non-public information that is required to accomplish official duties. NASA Users shall access, store, process, transmit or receive non-public NASA data only on authorized NASA devices, as specified in 1.1.d above. Special handling may be required for data that is protected under export control and ITAR, as well as any personally identifiable information (PII) or controlled unclassified information (CUI). NASA Users are responsible for ensuring that any CUI stored on a NASA device is handled in accordance with NPR 2810.7.

b. NASA Users shall use an OCIO-authorized and secured access method, e.g., NASA VPN and/or other OCIO-approved secure access method, to access non-public NASA data remotely.

c. NASA Users shall never use elevated privilege accounts for general user functions nor to access corporate resources, i.e., SharePoint, O365, etc. If necessary, workstation admin access, as described in NASA-SPEC-2675, will be provisioned and shall only be used in short durations to accomplish the required task.

d. If a non-loaner device is approved to be used outside the U.S., NASA users shall back up the device prior to travel. This back up is critical for data identification and recovery in the event of compromise, loss, theft, etc. of the traveler's device.

1.3 Use of NASA Information Technology Devices while Outside the U.S.

a. NASA Users shall physically take (or mail) only the minimum amount of IT devices required to accomplish official duties outside the U.S.

i. NASA Users shall attain Center Export Control approval to physically take (or mail) devices approved for use outside the U.S.

b. NASA Users shall use NASA IT devices for official business and shall not share them with unauthorized individuals.

i. If multiple NASA Users want to share a single OCIO WCS-provided loaner laptop device, please ensure this need is conveyed to the ESD Help Desk so that multiple user profiles can be configured on the loaner laptop.

c. Prior to any travel outside the United States with NASA IT devices, NASA Users shall have official approval. NASA users shall then initiate the prescribed ESD Service Request (see 2.1.d below in this directive) to request to take such a device outside the United States. The ESD Service Request will guide the NASA User and other organizations through the request, clearance, and approval process regarding the device and NASA information on the device. No devices may travel outside the United States unless this process has been completed successfully.

d. NASA users can travel with their assigned/issued NASA IT device to all countries EXCEPT for Russia or countries identified within the Designated Country List (DCL), as long as the machine has implemented all pertinent Agency technical standards and specifications for configuration. This check will occur as part of the Service Request process directed above and travel with the device only becomes authorized when the check is successful, the service request process is complete, and the export letter authorizing travel outside the U.S. with the identified device is provided.

e. NASA Users shall use only authorized NASA IT devices to store, process, transmit or receive NASA information while operating outside the U.S. All IT devices used during travel outside the U.S. to Russia or countries listed in the DCL must comply with all NASA requirements for the protection of sensitive information as laid out in NASA-SPEC-2675.

f. NASA Users shall not use personally-furnished equipment to store, process, transmit or receive non-public NASA data while operating outside the U.S. NASA Users of personally owned devices with the NASA Mobile Device Management (MDM) application installed shall not access the MDM application while outside the U.S. The MDM application must be uninstalled and unregistered from the NASA user's device prior to travel.

g. NASA Users shall only use OCIO WCS-provided Loaner Devices when on travel to or from Russia or a country on the DCL. These devices are configured with enhanced security standards to mitigate technical and operational risks of international travel to these countries.

i. OCIO Cybersecurity & Privacy Division (CSPD) Cybersecurity Standards and Engineering (CS&E) is responsible to create and maintain enhanced security

specifications and/or standards in response to the evolving cyber threat. These standards/specifications include the minimum requirements to use strong phishing-resistant multifactor authentication (MFA) and Data-at-Rest (DAR)/Data-in-Transit (DIT) encryption enabled with any NASA device used outside the U.S. that will travel to or from Russia or a country on the DCL.

h. NASA Users shall not connect authorized NASA IT devices to any non-NASA devices (e.g., removable media, smartphone, etc.) which are purchased, provided, or issued while outside of the U.S (with the exception of connecting removable storage media to presentation systems as explained below). The use of other U.S. Government resources is permitted for operational necessity.

i. When required to connect authorized NASA IT removable storage media to a presentation system, e.g., projector, display screen, NASA Users shall not reconnect the removable media to any other NASA device or system unless they have been cleared as indicated below.

ii. When information is provided, e.g., presentations via NASA IT removable media, these removable media devices must be cleared by the NASA Security Operations Center (SOC) Cybersecurity Incident Response Team (CIRT) upon reintegration and shall not be connected to the authorized NASA IT device until they have been cleared.

iii. NASA Users shall not connect a device to public USB charging outlets (such as those in airports, hotel lobbies, etc.) Instead, NASA Users should always use electrical power outlets for charging a device.

i. NASA Users shall, upon return from travel outside the U.S., surrender all OCIO WCS-provided loaner devices back to the ESD.

i. All loaner devices shall be surrendered within one business day of return. This cannot be waived.

ii. All loaner devices that have returned from Russia or a country on the DCL shall not access any NASA network to include on-premise, wireless, VPN, Mission network, etc. until cleared by OCIO WCS or the NASA SOC CIRT.

iii. All loaner devices received by the ESD shall be wiped and reloaded with a new fresh image.

1.4 Maintain Positive Control of NASA Information Technology Devices while Outside of the U.S.

a. NASA Users shall ensure all NASA IT devices and NASA information remain in their possession and are appropriately safeguarded at all times while outside the U.S.

b. NASA Users shall not:

i. Store authorized NASA IT devices in checked luggage.

ii. Leave devices unattended in vehicles.

iii. Leave devices unattended in public areas, i.e., airports, restaurants, conference rooms.

iv. Allow unauthorized users to use the device (includes mobile hotspots).

v. In any other way lose positive control of authorized NASA IT devices.

c. NASA Users traveling outside the U.S. with an authorized NASA IT device shall adhere to the following requirements when engaged or interfered with by U.S. Government or Foreign Government Authorities while traveling outside the U.S., specifically when entering or exiting sovereign borders.

d. U.S. Government and Foreign Government authorities may include but are not limited to; U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), and/or their foreign country equivalent.

i. If U.S. Government or Foreign Government authorities confiscate or attempt to confiscate a NASA-issued IT device, the NASA User shall show their NASA credentials and request to retain custody and control of the device, noting that the device in question is the property of the U.S. Government.

ii. If U.S. Government or Foreign Government authorities insist on examining or confiscating the device, the NASA User shall comply with the request to surrender the device.

iii If U.S. Government or Foreign Government authorities request access information for the NASA IT device, such as user identification or password, the NASA User shall restate their official status and that the device in question is the property of the U.S. Government.

iv. If U.S. Government or Foreign Government authorities insist on device access information, the NASA User shall request to input the information directly onto the device. If required, NASA personnel shall provide the access information to the U.S. or foreign authorities.

v. NASA Users shall request the return of the NASA IT device following the surrender and examination of the device by the U.S. Government or Foreign Government authorities.

vi. If the device is returned following the occurrence of any of the incidents above, the NASA User shall power off the device and not power the device on again except for emergency contact purposes. The device shall not **connect to** a NASA system or network until cleared by the NASA SOC CIRT.

e. The NASA User shall contact the NASA SOC**, soc@nasa.gov, or call 877-627-2732** and supervisor immediately, but no longer than 24 hours after any of the following incidents:

i. If the NASA User is unable to maintain positive control of the authorized IT device

ii. If the device lost, stolen, damaged, or suspected to have been tampered with

iii. If any of the incidents described above in this paragraph 1.4 occur

iv. Unusual or suspicious activity by the device or operating system.

f. In addition to the SOC, a NASA User shall contact **NASA Counterintelligence (NASA CI) counterintelligence@nasa.gov** immediately, but no longer than 24 hours after any of the following incidents:

i Attempts by any foreign nationals or representatives of a foreign Government to possess or access NASA IT devices or information.

ii. Unusual or suspicious overtures by any foreign entity to acquire NASA CUI or other sensitive information outside established official channels.

Chapter 2. Responsibilities

2.1 NASA OCIO Roles and Responsibilities

a. The NASA Chief Information Officer shall maintain, review, and update this NID as well as subsequent NPR and other related policies.

b. The NASA Senior Agency Information Security Official (SAISO) shall;

i. Enforce guidance provided throughout the directive, to include final approval process for whether a NASA IT device can travel outside the U.S.

ii. Maintain, review and update this directive and complementary directives as appropriate

iii. Develop and disseminate guidance and standards on safeguarding NASA IT devices to NASA Users while outside the U.S.

iv. Approve baseline and enhanced security standards commensurate with the cybersecurity threat and risk assessment

v. Provide guidance and direction for handling cybersecurity incidents while outside U.S.

c. The WCS Service Line Director, or designees, shall:

i. Ensure that OCIO WCS-provided loaner devices are available and are properly configured for NASA use while on international travel to Russia or countries on the DCL.

ii. Wipe and restore all OCIO WCS-provided loaner devices upon return from travel outside the United States.

d. The Cybersecurity Services (CyS) Service Line Director or their designees shall:

i. Create and maintain an ESD Service Request that guides a NASA User through the request and approval process prior to taking any NASA IT device outside the United States.

Ii. Ensure the technical ability to conduct compliance checks of devices requested to travel outside the United States as part of the Service Request workflow.

Iii. Coordinate the Service Request workflow with Export Control and NASA CI.

2.2 NASA User Roles and Responsibilities

2.2.1 NASA Users shall:

a. Adhere to the responsibilities outlined throughout this directive

b. Follow all supporting processes and adhere to prescribed timelines. In the absence of process or applicable guidance, contact the ESD for guidance.

c. Ensure that their NASA issued device has implemented all pertinent Agency technical standards and specifications for configuration (in particular that it is multifactor (MFA) and Data-at-Rest (DAR)/Data-in-Transit (DIT) encryption enabled) by completing the designated service request process prior to travel. NOTE: this is applicable to all devices addressed by this policy.

e. Travel with adequate NASA-provided power cords, chargers, adapters, etc., to prevent the need to purchase or use peripherals in the host country.

2.3 NASA Security Operations Center (SOC) Roles and Responsibilities

2.3.1 The NASA SOC shall:

a. Open a NASA security incident ticket for any detected access from outside the U.S. and U.S. territories, including at points of entry/exit by any U.S. Customs and Border Protection (CBP) or foreign country border officials, to any NASA systems, networks, and data not intended for access by the general public by any NASA user whose travel information is not on file with the NASA SOC.

b. Notify the NASA Counterintelligence (CI) Office of any incursion opportunities or activity or confirm with CI that the NASA user has already made an adequate report.

c. Maintain travel information in a secure repository accessible to Center CISOs, Incident Response Teams, and other authorized NASA personnel who require travel information.

d. Utilize the SOC's Cybersecurity Incident Response Team (CIRT) to review NASA IT loaner devices returning from international travel to countries on the DCL and ensure all required mitigation actions (currently scanning, wiping, and re-imaging the hard drive or mobile device to a known good state) are taken prior to authorizing the re-connection of the NASA IT devices directly within the Trusted Internet Connection NASA Authorization boundary.

Appendix A: Definitions

Controlled Unclassified Information. Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

NASA Device. A system, object, or intellectual property created by a NASA employee or contractor or any combination thereof, owned by NASA, to include information, records, data, information technology systems, and applications.

NASA Information. NASA information is defined as any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for or is under the control of NASA.

Non-Public Information. NASA non-public information includes all known categories of CUI and information otherwise assessed as SBU information and classified information.

Appendix B: Acronyms

CBP	Customs and Border Protection
CFR	Code of Federal Regulation
CIO	Chief Information Officer
CIRT	Cybersecurity Incident Response Team
CISO	Chief Information Security Officer
CSPD	Cybersecurity & Privacy Division
CUI	Controlled Unclassified Information
DAR	Data-at-Rest
DCL	Designated Country List
EAR	Export Administration Regulations
ESD	Enterprise Service Desk
FFRDC	Federally Funded Research and Development Center
FISMA	Federal Information Security Modernization Act
GFP	Government Furnished Property
HBK	Handbook
IT	Information Technology
ITS	Information Technology Security
ITAR	International Traffic in Arms Regulations
JPL	Jet Propulsion Laboratory
MDM	Mobile Device Management
MFA	Multifactor Authentication
NAII	NASA Advisory Implementing Instruction
NPR	NASA Procedural Requirements

OCIO	Office of Chief Information Officer
PII	Personally Identifiable Information
SAISO	Senior Agency Information Security Official
SOC	Security Operations Center
TSA	Transportation Security Administration
USB	Universal Serial Bus
WCS	Workplace and Collaboration Services