NASA Policy Directive

NPD 2540.1K
Effective Date: August 11, 2022
Expiration Date: August 11, 2027

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. It is NASA policy to:

(1) Permit limited acceptable personal use of NASA Government-furnished property (GFP), information technology (IT) equipment, services, and resources (hereinafter referred to as NASA IT) for non-government purposes, when such use does not overburden any of the Agency's IT services and resources and when access to these IT services and resources does not interfere with official Government business. GFP includes NASA assets, including all devices and equipment. The intent of limited acceptable personal use is to provide a professional and supportive work environment while meeting taxpayer expectations that tax dollars be spent wisely. Acceptable personal use is limited to use that incurs no more than minimal additional expense to the Government in areas such as: communications infrastructure costs; use of consumables in limited amounts; general wear and tear on property; minimal data storage on storage devices; and minimal impacts on NASA IT systems.

(2) Permit limited acceptable personal use of NASA GFP, IT equipment, services, and resources to individuals during the non-duty time of reasonable duration and frequency of use, including during official work breaks, and when the use does not:

(a) adversely affect the performance of official duties;

(b) result in the loss of an individual's productivity;

(c) pose a cybersecurity risk;

(d) violate applicable laws and regulations; or

(e) interfere with the official business or mission of NASA.

(3) Not allow NASA equipment to be used to download illegal, inappropriate, or unauthorized content and untrusted, unapproved, or malicious software applications or services. Use of NASA IT is prohibited for commercial purposes, "for-profit" and "non-profit" activities, or in support of outside employment or business activity.

(4) Maintain that individuals have no expectation of privacy while using any NASA IT at any time, including, but not limited to accessing the Internet, proxy-bypass services, or e-mail. Users have no expectation of privacy even during limited periods of personal use. They have no expectation of privacy even when using personal equipment, services, and applications while connected to NASA GFP, IT equipment, or services.

(5) Maintain that non-compliance or unauthorized or improper use of NASA IT may result in the suspension or revocation of access to NASA products, networks and services, disciplinary action, as well as civil and criminal penalties. Unauthorized and improper use is defined in Attachment C.

(6) Maintain that Authorizing Officials (AOs) for mission systems may impose stricter security controls, user privacy controls, and restrict applications for their systems due to mission criticality or unique mission requirements.

(7) Maintain that the privilege to use NASA GFP, IT equipment, services, and resources for non-government purposes may be revoked or limited at any time by Federal or Agency officials. NASA Centers and contractors may

invoke stricter policies or implementing guidance.

2. APPLICABILITY

a. This directive applies to NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers. For purposes of this directive, NASA Headquarters is treated as a Center. Further, all stipulated Center requirements apply to NASA Headquarters.

b. This directive applies to contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the contracts, grants, or agreements. This directive is applicable to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), only to the extent specified in the NASA/Caltech Prime Contract.

c. This directive applies to all unclassified NASA information and NASA information systems, including those that are contracted out, outsourced to, or operated by:

(1) Government-owned, contractor-operated (GOCO) facilities;

(2) partners under the National Aeronautics and Space Act; 51 U.S.C. § 20101, et seq;

(3) partners under the Commercial Space Launch Act, as amended, 51 U.S.C. § 50913;

(4) partners under cooperative agreements; or

(5) commercial or university facilities.

d. In this directive, 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.

e. This directive applies to NASA IT User acceptable use of NASA GFP, approved non-GFP, NASA IT, and personally owned IT devices (including Internet of Things (IoT) devices) when connected to NASA GFP, IT equipment, services, resources, and NASA data. Additional policies and procedures on contractor-accountable, NASA-owned, and Center-accountable property can be found in Federal Acquisition Regulation (FAR), Government Property, 48 CFR pt. 45; NASA FAR Supplement, Government Property, 48 CFR 1800, pt. 1845; and the terms and conditions of individual contracts.

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

3. AUTHORITY

a. Federal Information Security Modernization Act of 2014, 44 U.S.C. §3551.

b. Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems.

4. APPLICABILITY DOCUMENTS AND FORMS

a. NPD 2810.1, NASA Information Security Policy.

b. NPR 1382.1, NASA Privacy Procedural Requirements.

c. NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

d. ITS-HBK-SCRM.2810.v1.0.0, Information & Communications Technology Supply Chain Risk Management.

e. NASA Advisory Implementing Instruction 1050-3B, NASA Partnerships Guide.

5. RESPONSIBILITY

a. The Office of the Chief Information Officer (OCIO) shall:

(1) Implement, manage, and maintain this directive, and ensure this policy is disseminated to all NASA IT Users.

(2) Ensure sufficient controls at the Agency level and procedures for NASA IT Users' awareness of proper personal use of GFP and non-GFP (including personally owned devices) when connected to NASA networks, IT equipment, and services and are responsible for developing cost-effective controls for monitoring or preventing abnormal or

inappropriate use. GFP controls include blocking of inappropriate websites and phone numbers, flagging abnormal long distance or other phone charges, and monitoring network traffic for suspicious traffic or inappropriate use (see Attachment C.2 for definition).

b. Information System Owners (ISOs) shall:

(1) Ensure that current NASA interns, partners, grantees, and other users covered under Space Act Agreements or other official NASA agreements are knowledgeable of Federal and Agency policy before using U.S. Government property, data, and services.

(2) Authorize limited installation of software necessary for mission functions with the documented approval of the system AO.

(3) Ensure that software authorized per 5.b(2) above:

(a) meets supply chain requirements identified in ITS-HBK-SCRM.2810.v1.0.0, Information & Communications Technology Supply Chain Risk Management;

(b) is licensed for NASA use; and

(c) is obtained from a safe and authorized source per the procedures described in ITS-HBK-SCRM.2810.v1.0.0.

(4) Request the minimum software installation necessary for mission functions, in coordination with the Center IT Asset Manager (ITAM). A list of ITAMs is available at: https://www.nssc.nasa.gov/elmt.

c. Current NASA interns, partners, grantees, and other users covered by Space Act Agreements or other official NASA agreements may use NASA GFP, IT equipment and services consistent with their agreements if explicitly authorized by the applicable ISO.

d. Contracting Officers, as defined in Federal Acquisition Regulation 2.101, or Agreement Managers, as defined in NASA Advisory Implementing Instruction 1050-3B, NASA Partnerships Guide, shall:

(1) Ensure that contractors are informed on the uses of Government IT resources, approved/authorized non-GFP, and personally owned devices as a part of the introductory IT security training, orientation, or the implementation of this policy as part of a NASA contract.

(2) Ensure that contractors address allowable use of Government IT resources in System Security Plans, IT Security Plans, and IT Security Management Plans.

(3) Ensure contractors who process, store, or transmit NASA information on approved/authorized non-GFP or personally owned devices, IT equipment, software, and media do so only when the contract under which they perform specifically establishes terms and conditions for such use, that necessary approvals have been obtained, and that the contractor otherwise meets and complies with NASA security standards and policy.

e. Supervisors shall:

(1) Permit the allowable use of NASA IT equipment, services, and resources.

(2) Pursue sanctions for misuse of NASA IT, including potential disciplinary action.

(3) Ensure NASA IT Users taking NASA IT equipment outside the U.S., whether on official or personal travel, meet the requirements in accordance with NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

(4) Ensure NASA IT Users taking NASA IT equipment outside of the U.S. have export authorization, which includes validation of official work requirement for the employee or contractor that necessitates exporting GFP or IT equipment in support of Government business.

f. NASA IT Users shall:

(1) Comply with the requirements regarding personal use of NASA IT equipment, services, and resources and the Rules of Behavior for U.S. Government property, data, and services as outlined here and in Attachments C (Specific Provisions) and G (Rules of Behavior) to this directive.

(2) Have no expectation of privacy whether using NASA GFP or Non-GFP (employee's own personally supplied property), including, but not limited to, Internet access, proxy-bypass services, or e-mail, even during limited periods of personal use.

(3) Ensure that the personal use is consistent with Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR pt. 2635, if civil servants.

(4) Conduct themselves professionally in the workplace and not use NASA IT for activities that are inappropriate or illegal (see Attachment C.2).

(5) Ensure that the personal use of NASA IT does not create the appearance of acting in an official capacity or that NASA endorses or sanctions any personal activities.

(6) Separate official and personal communications to ensure all official communications are identified and conducted to comply with applicable law, regulation, and policy.

(7) When using NASA IT, use social media responsibly, safely, and judiciously, whether in an official capacity or for personal use, to protect mission objectives, information assets, program integrity, data, and NASA's reputation.

(8) Not alter or change in any way configurations for NASA IT in a manner that does not adhere to NASA policy, specifications, or standards.

(9) Not use NASA IT to download illegal, inappropriate, or unauthorized content or untrusted, unapproved, or malicious software applications or services.

(10) Not use NASA IT for commercial purposes, "for profit" and "non- profit" activities, or for outside employment or business activity, such as a sole proprietorship.

(11) Not download, copy, or install unapproved or unauthorized software applications or data programs onto NASA IT or NASA-approved and authorized networks and devices, including, but not limited to:

(a) Screen savers.

(b) Computer games.

(c) Personal financial management software.

(d) Tax preparation software.

(e) Free, test, trial, or demo software.

(f) "Push" technology applications.

(g) Network monitoring software.

(h) Video-conferencing software.

(i) Virtual machines.

(12) Not engage in prohibited activities on NASA IT or NASA-approved and authorized networks and devices, including, but not limited to:

(a) Peer-to-peer (P2P) file sharing.

(b) Online file storage using services not explicitly authorized by NASA.

(c) Online gaming or gambling.

(d) Cryptocurrency-mining.

(e) Installing, viewing, or accessing the following types of software or websites:

(i) Pornographic, sexually explicit, or sexually oriented materials.

(ii) Personal services websites, such as dating services where a user registers NASA credentials creating an appearance that the user is acting in an official capacity or with NASA's endorsement.

(iii) Hacking-related websites or sites which expose NASA to unacceptable security risk regardless of the known or potential security risks or lack thereof.

(iv) Proxy-bypass services, or services of similar capabilities. See Attachment E.

(v) Unauthorized remote access sites, software, or services of similar capabilities. See Attachment E.

(13) Not install software created or maintained by companies banned by the Federal Government on NASA IT, services or resources, or on any system storing, transmitting, or processing NASA data. See Attachment F.

(14) Not connect by any method equipment manufactured by companies banned by the Federal Government to NASA IT, services or resources, or on any system storing, transmitting, or processing NASA data. See Attachment

F.

(15) Not use equipment manufactured by companies banned by the Federal Government for any Government or non-government business use including but not limited to hardware, telecommunications, data storage, data processing, or video or voice communications. Federal Government has banned the equipment of the following companies that manufacture them:

1. Telecommunications equipment produced by Huawei Technologies Company, including telecommunications or video surveillance services provided by such entity or using such equipment.

2. Telecommunications equipment produced by ZTE Corporation, including telecommunications or video surveillance services provided by such entity or using such equipment.

3. Video surveillance and telecommunications equipment produced by Hytera Communications Corporation, to the extent it is used for the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

4. Video surveillance and telecommunications equipment produced by Hangzhou Hikvision Digital Technology Company, to the extent it is used for the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

5. Video surveillance and telecommunications equipment produced by Dahua Technology Company, to the extent it is used for the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

6. Information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates.

7. International telecommunications services provided by China Mobile International USA Inc., subject to section 214 of the Communications Act of 1934.

8. Telecommunications services provided by China Telecom (Americas) Corp. subject to section 214 of the Communications Act of 1934.

9. Detailed and updated information can be found at https://www.fcc.gov/supplychain/coveredlist. This prohibition applies to:

(a) All business uses and infrastructure, including those not tied to Government or its data.

(b) Any and all Bring Your Own Device (BYOD) programs, meaning all banned equipment cannot participate in any contractor BYOD programs.

(c) All contractor's IT equipment, services, or resources including corporate, visitor, test, stage, production, stand-alone; prohibited telecommunications equipment cannot connect to any contractor-owned, managed, or out-sourced network or system.

(d) Connecting any contractor IT equipment, services, or resources to any equipment, personally owned or otherwise, that uses or is equipment banned by the Federal Government.

(16) Not connect any personal device, used wholly and entirely for personal use, to NASA network when they are on the premises of a NASA Center, facility, campus, or any type of NASA property.

(17) Access the NASA Visitor Network only:

(a) for non-NASA purposes;

(b) using NASA Domain Name System (DNS) servers; and

(c) using Hypertext Transfer Protocol (HTTP) over Transport Layer Security (HTTPS).

(18) Not access the NASA Visitor Network using NASA IT.

(19) Not use personally owned equipment to access NASA IT, except as explicitly authorized by the NASA CIO. See Attachment C.

(20) Not connect unauthorized non-NASA devices to NASA IT via Universal Serial Bus (USB), Bluetooth, or any other connection methods.

(21) Not connect NASA IT via any method to any non-NASA IT that provides data storage, including, but not limited to USB or "thumb drive" external storage devices, external hard drives, smartphones, tablets, and cameras.

(22) Notwithstanding f(20) above, connect NASA IT assigned to them to the following acceptable personally owned non-NASA devices through wired or wireless connections, when conducting Government business remotely and if such equipment is not manufactured by companies banned by the Federal Government (see Attachment F).

(a) A personally owned monitor.

(b) A personally owned keyboard.

(c) A personally owned mouse.

(d) A personally owned scanner.

(e) A personally owned printer.

(f) A personally owned home network router.

(g) A personally owned headset or hands-free audio device.

(h) Personally owned headphones.

(i) A personally owned webcam.

(23) Remove NASA IT from the workplace for official business only.

(24) Use NASA IT equipment outside of the workplace for official business and ensure that the equipment:

(a) remains in their custody;

(b) is handled and maintained properly, and

(c) is returned in good condition.

(25) Notify their supervisor, the NASA Security Operations Center at soc@nasa.gov or 877-NASASEC (877-627-2732), and their respective Center Physical Security office immediately when NASA IT is lost, stolen, or damaged.

(26) Users of JPL FFRDC NASA IT shall report incidents to the JPL Security Operations Center (SOC) according to local user guidance agreed to between NASA and the contractor operating the JPL FFRDC.

6. DELEGATION OF AUTHORITY

None.

7. MEASUREMENT/VERIFICATION

ISOs may access any electronic communications conducted via NASA IT and services and employ monitoring tools to detect improper use. ISOs or their designees determine, implement, ensure, and document compliance by applying a verification approach tailored to meet the requirements of this directive. The Office of Protective Services conducts functional reviews, spot checks, and inspections to review compliance and implementation. The ISO has enterprise tools on their systems to detect unauthorized access.

8. CANCELLATION

NPD 2540.1I, Personal Use of Government Office Equipment Including Information Technology, August 19, 2019.

NID 2540.138, Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources, August 18, 2021.

/s/ Bill Nelson
Administrator

ATTACHMENT A: Definitions

Authorization to Operate (ATO) - the formal acceptance, by an AO, that the security of an information system's

operation is commensurate with the risk and magnitude of harm resulting from a compromise of that system's confidentiality, integrity, and availability.

Authorizing Official (AO) - a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, individuals, other organizations, and the Nation.

Government-Furnished Property (GFP) - property owned or leased by the Federal Government and includes Government office property that is property in the possession of, or directly acquired by, the Government and can be subsequently furnished to the contractor for performance of a contract.

GFP also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. (FAR, Part 45.101) This also includes property provided for use while in official travel status, provided for telework, or other alternative workspace arrangements. GFP includes, but is not limited to:

a. computers and related peripheral property.

b. software.

c. library resources.

d. research or reference services (e.g., online journals).

e. telephones and wireless communications devices (e.g., cell phones, smartphones, pagers.)

f. personal electronic devices (e.g., calculators, music players, global, positioning system devices, book readers).

g. facsimile machines.

h. photocopiers.

i. office supplies.

j. Government guest networks.

k. network access (e.g., Internet, wireless, cellular).

l. e-mail.

m. licenses (e.g., software licenses).

Information System Owner - the principal advisor to the Center Chief Information Security Officer (CISO) on matters pertaining to specific information systems according to NPR 1382.1, NASA Privacy Procedural Requirements.

Information Technology - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the Agency. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Technology (IT) User - is any employee, contractor employee, or any other individual authorized to access or use NASA IT.

NASA Information - per NPD 2810.1, NASA Information Security Policy, any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of NASA.

Network - a system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Personally owned device - includes but is not limited to any device such as a phone, tablet, laptop, personal computer, IoT device, or wearable technology that does not have a valid ATO from a NASA AO.

Personal use - use other than for official Government business.

Peer-to-Peer file sharing - as defined in OMB M-04-26, Personal Use Policies, file sharing technology, refers to any software or system allowing individual users of the Internet to connect to each other and trade files.

Privilege - NASA is extending the opportunity to its IT Users to use GFP for limited personal use to create a more supportive work environment. NASA IT Users have no inherent right to personal use or ownership of GFP. The

personal use privilege does not extend to modifying GFP, including modifications such as loading personal software or making configuration changes, or other changes that are inconsistent with Agency policy.

Property - a tangible asset, end item, or nonexpendable property that is functionally complete, not intended for sale, does not lose its identity, or become a component part of another item when put into use. Property is not intended to be destroyed during an experiment and has a useful life of two years or more. Proxy-Bypass Service - is a service used to bypass specific cybersecurity elements implemented in firewalls and proxies by bypassing security controls used to restrict or manage access.

Push Technology - is a style of Internet-based communication where the request for a given transaction is initiated by the publisher or central server. A user "subscribes" to various information "channels" provided by a server; whenever new content is available on one of those channels, the server pushes that information directly to the user's system without any request action being taken by the user.

Social media - includes, but is not limited to, wikis, blogs, mash-ups, Web feeds (e.g., Really Simple Syndication and Rich Site Summary (RSS) feeds), social networking sites (e.g., Facebook), microblogging (e.g., Twitter), and Web-based forums.

Unapproved or Unauthorized Software or Services - are applications and IT services that do not have a NASA ATO or have not been approved for use by NASA. This includes Federal Risk and Authorization Management Program (FedRAMP) services that have not completed the NASA Assessment and Authorization process. Attachment B. Acronyms

AO Authorizing Official

ATO Authorization to Operate

CFR Code of Federal Regulations

CIO Chief Information Officer

CISO Center Chief Information Security Officer

DNS Domain Name System

E.O. Executive Order

FAR Federal Acquisition Regulation

FedRAMP Federal Risk and Authorization Management Program

GFP Government-Furnished Property

HBK Handbook

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol over Transport Layer Security

IoT Internet of Things

ISO Information System Owner

IT Information Technology

ITAM Information Technology Asset Manager

ITS Information Technology Security

NASA National Aeronautics and Space Administration

NID NASA Interim Directive

NPD NASA Policy Directive

NPR NASA Procedural Requirement

OCIO Office of the Chief Information Officer

OMB Office of Management and Budget

OPS Office of Protective Services

P2P Peer-to-Peer

SOP Standard Operating Procedure

USB Universal Serial Bus

U.S.C. United States Code Attachment C. Specific Provisions

C.1. Employees and contractors are permitted limited personal use of GFP and IT services to the extent that such personal use does not interfere with official duties or result in a loss of productivity and for contractors only to the extent specified or referenced in their contracts. Employees and contractors are only authorized to use office property and services for personal use if they are first authorized to use the property for official business. NASA is not required to supply property if the property is not required for the employee or contractor to perform official business. Moreover, personal use may incur only minimal additional expense to the Government in areas such as:

a. Communications infrastructure costs such as, but not limited to, telephone or data charges, Internet connectivity, and telecommunications traffic.

b. Consumables such as, but not limited to, paper, ink, and toner.

c. Wear and tear on property such as, but not limited to, copiers and printers.

d. Impacts on network bandwidth such as, but not limited to, e-mail message sizes, e-mails with attachments, text messaging, and personal use of social media (e.g., Twitter, Facebook, and YouTube).

C.2. Inappropriate Personal Use - Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using GFP and IT services for activities that are inappropriate. Misuse or inappropriate use of GFP and IT services includes, but is not limited to:

a. Any personal use that violates applicable law, regulation, Federal or Agency policies, or procedural requirements.

b. Any personal use of unauthorized streaming media services (or other software or services that could cause unnecessary congestion, delay, or disruption of service to any Government system or component). Examples include, but are not limited to, Netflix, SiriusXM, Amazon Prime Video/Music, Pandora, Spotify, Disney+, YouTube TV, or any other similar services.

c. Using a Government system as a staging ground or platform to gain unauthorized access to other systems.

d. The creation, copying, transmission, or retransmission of unauthorized mass mailings, regardless of subject matter.

e. Activities inconsistent with 5 CFR pt. 2635.

f. Accessing, sharing, posting, storing, or copying material that is inappropriate or offensive based on race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, gender identity, or status as a parent.

g. Creating, searching/downloading, viewing, storing, copying, or transmitting materials describing or depicting sexually explicit conduct, or other sexually explicit or sexually oriented materials.

h. Use for commercial purposes, "for profit" activities, or in support of outside employment or business activity such as a personal business or assisting friends, relatives, or others in such activities (e.g., consulting for pay, sales, or administration of business transactions, and sale of goods or services, unless on authorized bulletin boards provided by the Agency).

i. Engaging, in a personal or private capacity, in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature).

j. Publicly communicating Agency information, including Agency policy, project, or program information and other critical data, that does not concern a protected disclosure under Title 5, U.S.C., Government Organization and Employees, or that has not been authorized for release. This includes uses that could create the perception that the communication was made on behalf of the Agency or the Office of the Administrator if the communication has not been authorized by the Office of Communications. Authorized public communications of Agency information are subject to Release of Information to News and Information Media, 14 CFR pt. 1213, and applicable Agency policies.

k. Any use that could generate more than minimal additional expense to the Government.

l. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information,

including computer software and data, that includes privacy, copyrighted, trademarked information, or material with other intellectual property rights (such as literature, music, and videos beyond fair use), proprietary data, or export-controlled software or data.

m. Participation in P2P file sharing activities or use of such software including, but not limited to, BitTorrent, uTorrent, Gnutella, and Vuze.

n. Overriding or defeating a security feature of a Government system (e.g., installing unapproved software or jailbreaking).

C.3. Privacy Expectations - NASA employees and contractors do not have a right to expect privacy while using Government office property or IT services at any time, including accessing the Internet and using e-mail. Employees and contractors are advised that the Government maintains call detail and network access records to monitor telephone activity and Internet access and employs monitoring tools to track system performance and improper use. To the extent that employees and contractors wish their private activities to remain private, they need to refrain from personal use of GFP and IT services. By using GFP, employees and contractors consent to disclosing the contents of any files or information maintained on or passed through the property. Any use of Government communication resources are made with the understanding that such use is subject to Government surveillance and inspection in accordance with the law, is not private, and is not anonymous. This includes personal property (e.g., tablets, smartphones) that connect to Government networks and services.

C.4. Sanctions for Misuse - Unauthorized or improper use of GFP and IT services could result in loss of use or limitations on the use of property, disciplinary or adverse personnel actions, criminal penalties, and/or employees/contractors being held financially liable for the cost of improper use. Attachment D. References

D.1. Government Organizations and Employees, 5, U.S.C.

D.2. The Hatch Act, 5 U.S.C. § 7323.

D.3. Definitions, 40 U.S.C. § 11101(6).

D.4. The National Aeronautics and Space Act; 51 U.S.C. § 20101, et seq.

D.5. The Commercial Space Launch Act, as amended, 51 U.S.C. § 50913.

D.6. Office of Personnel Management, Employee Responsibilities and Conduct, 5 CFR pt. 735.

D.7. Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR pt. 2635.

D.8. Supplemental Standards of Ethical Conduct for Employees of the National Aeronautics and Space Administration, 5 CFR pt. 6900.

D.9. Release of Information to News and Information Media, 14 CFR, pt. 1213.

D.10. Federal Acquisition Regulation, Government Property, 48 CFR pt. 45.

D.11. NASA FAR Supplement, Government Property, 48 CFR pts 1800 and 1845.

D.12. Principles of Ethical Conduct for Government Officers and Employees. Executive Order (E.O.) 12674 of April 12, 1989, as amended by E.O. 12731 of October 17, 1990.

D.13. Federal Information Technology, E.O. 13011 of July 16, 1996, as amended by E.O. 13284 of January 23, 2003, and E.O. 13286 of February 28, 2003.

D.14. OMB M-04-26, Personal Use Policies and "File Sharing" Technology.

D.15. OMB M-10-23, Guidance for Agency Use of Third-Party Web sites and Applications.

D.16. OMB M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements.

D.17. NPD 1900.9, Ethics Program Management.

D.18. NPR 1900.3, Ethics Program Management.

D.19. NPR 2810.1, Security of Information and Information Systems.

D.20. NPR 3600.2, NASA Telework Program.

D.21. NPR 4200.1, NASA Equipment Management Procedural Requirements.

D.22. NASA Information Technology Security Handbook (ITS-HBK) 2810.07-01, Configuration Management.

D.23. ITS-HBK-2810.15-01, Access Control.

D.24. ITS-HBK-2810.17-01, Identification and Authentication.

D.25. NASA IT Rules of Behavior, 10 Oct 2020.

D.26. NASA ITS-SOP 2810.01A, Collection of Electronic Data. Attachment E. Examples

E.1. Examples of Proxy-Bypass Services: 3Proxy, Unblockme, and Proxite.

E.2. Examples of unauthorized remote access protocols, sites, or software: Telnet, virtual network computing, X11 (when configured to allow remote access), LogMeIn, TeamViewer, Chrome Remote Desktop, GoToMyPC, Apple Remote Desktop, BeAnywhere, ShowMyPC, and any non-NASA issued VPN software. Attachment F. Banned Companies

Federal Government has banned the equipment of the following companies that manufacture them:

F.1 Telecommunications equipment produced by Huawei Technologies Company, including telecommunications or video surveillance services provided by such entity or using such equipment.

F.2 Telecommunications equipment produced by ZTE Corporation, including telecommunications or video surveillance services provided by such entity or using such equipment.

F.3 Video surveillance and telecommunications equipment produced by Hytera Communications Corporation, to the extent it is used for the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

F.4 Video surveillance and telecommunications equipment produced by Hangzhou Hikvision Digital Technology Company, to the extent it is used for the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

F.5 Video surveillance and telecommunications equipment produced by Dahua Technology Company, to the extent it is used for the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.

F.6 Information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates.

F.7 International telecommunications services provided by China Mobile International USA Inc., subject to section 214 of the Communications Act of 1934. F.8 Telecommunications services provided by China Telecom (Americas) Corp. subject to section 214 of the Communications Act of 1934.

Detailed and updated information can be found at https://www.fcc.gov/supplychain/coveredlist.

RULES OF BEHAVIOR (NASA Access Only)

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.