National Aeronautics and
Space Administration
John C. Stennis Space Center
Stennis Space Center, MS 39529-6000

SPD 2800.3 Rev Basic-1
April 2016

COMPLIANCE IS MANDATORY

John C. Stennis Space Center
Policy Directive
Mobile Code

Document History Log

Status/Change/ Revision	Change Date	Originator/Phone	Description
Basic	June 2011	Monti Muhsin 8-2069	Initial Release
Basic-1	April 2016	Mitch Krell/8-1821	Administrative changes

1. POLICY

a. John C. Stennis Space Center (SSC) will restrict the use of unsigned external mobile code on servers, desktops and mobile devices. Mobile code refers to programs (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. The term also applies to situations involving a large homogeneous collection of platforms (e.g., Microsoft Windows). Mobile code is software that can be transferred through the network, e-mail, or ftp and executed on a local system without the knowledge of or interaction by the recipient. Examples of mobile code are as follows: Javascript and VBScript; Java applets; ActiveX Controls; Shockwave Movies; and Microsoft Office document macros.

b. The capability of executing external mobile code is restricted by implementing the U.S. Government Configuration Baseline (USGCB)(formerly Federal Desktop Core Configuration (FDCC)), Center for Internet Security (CIS) Benchmarks, NASA Agency configurations, and configuration of anti-virus clients.

c. Mobile code implemented within internal SSC applications is not currently restricted.

2. APPLICABILITY

The policy or policies defined herein apply to all NASA SSC employees, NASA SSC contractors, and to the extent appropriate Resident Agency organizations, in achieving NASA SSC and Agency missions, programs, projects, and institutional requirements. Specifically, the policies prescribed within this document apply to all offices under the management of the SSC Center Director. Other co-located offices are encouraged to adopt these policies to ensure compatibility with systems and processes.

3. AUTHORITY

a. 5 U.S.C. 552, et. seq., the Freedom of Information Act, as implemented by 14 CFR 1201.

b. 5 U.S.C. 552a, the Privacy Act of 1974, P.L. 93-579, as amended.

c. 18 U.S.C. 510, et. seq., the Electronic Communications Privacy Act, as amended.

d. 40 U.S.C. 759 note, the Computer Security Act of 1987, P L. 100-235, as amended.

e. 40 U.S.C. 140, et. seq., Section 808 of Public Law 104-208, the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Public Law 104-106].

f. 42 U.S.C. 2451, et. seq., the National Aeronautics and Space Act of 1958, as amended.

g. 44 U.S.C. 2510, et. seq., the Paperwork Reduction Act of 1995, P.L. 104-13, as amended.

h. Executive Order No. 13011, Federal Information Technology of July 16, 1996.

i. OMB Circular A-130, Management of Federal Information Resources, Appendix III.

j. NPD 2800.1, *Managing Information Technology*.

k. NPD 2810.1, *NASA Information Security Policy*.

Note: The above listed authorities are generally applicable to all IT network activities. The list is not necessarily all-inclusive; additional authorities, executive orders, notices, and directives may apply. In the case where other authorities are indicated, they will be noted within the specific appended subject policy.

4. APPLICABLE DOCUMENTS

a. ITS-HBK-2810.18-01, *Systems and Communications Protection Handbook*

b. NIST Special Publications SP 800-28 Version 2, G*uidelines on Active Content and Mobile Code*

c. NIST Special Publications SP 800-19, *Mobile Agent Security*

d. NIST SP 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

5. RESPONSIBILITY

a. Center Chief Information Security Officer (CISO). The CISO is responsible for the overall management of the SSC IT Security Program, providing Center information system policy and:

(1) Ensuring Information System Owners (ISO) have applied the Agency defined configuration baselines to all systems.

(2) Reviewing and approving the use of unsigned external mobile code on SSC systems.

b. Information System Owners (ISO). The ISOs are responsible for implementing Agency and Center policies and ensuring the appropriate security configurations are applied to the systems they are responsible for.

c. Information System Users. Information system users are responsible for following Agency and Center policies for the use of information systems assigned to them and notifying

appropriate offices (Desktop Support Help Desk or System Administrator) when warning "pop-ups" or other indications of possible unauthorized mobile code are encountered.

6. CANCELLATION

None

Signature on file

Patrick E. Scheuermann
Director

DISTRIBUTION
Approved for public release via NODIS and TechDoc; distribution is unlimited.

Acronyms

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CSO	Computer Security Officials
FDCC	Federal Desktop Core Configuration
HBK	Handbook
IT	Information Technology
ITS	Information Technology Security
NASA	National Aeronautics and Space Administration
NODIS	NASA Online Directives Information System
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
OMB	Office of Management and Budget
PL	Public Law
SP	Special Publication
SPD	Stennis Policy Directive
SSC	Stennis Space Center
U.S.C.	United States Code
USGCB	U.S. Government Configuration Baseline

Definitions

Center for Internet Security (CIS) Benchmarks: Recommended configurations to improve the security of systems and devices. These configurations have been tested and reviewed by organizations and security experts.

Mobile Code: Mobile code is software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded within Office documents.

Mobile Devices: Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), Universal Serial Bus (USB) port devices, Optical Disk Storage (Compact Discs (CDs) and Digital Versatile Discs (DVDs)), Cellular Phones (iPhones, iPads, Tablet PCs and Smart Phones), Digital Video Recorders, Digital Audio Recorders, MP3 Players (iPods), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or NASA owned, that may connect to or access the information systems at the Stennis Space Center.

Unsigned External Mobile Code: Mobile code provided by an external entity that is not digitally signed by a trusted certificate authority (e.g., VeriSign, Digicert, Trustwave, etc).

U.S. Government Configuration Baseline (Formerly Federal Desktop Core Configuration (FDCC)): An Office of Management and Budget initiative designed to create security configuration baselines for Information Technology products widely deployed across the federal agencies.