NNG13451284R

ATTACHMENT H

IT SECURITY
APPLICABLE DOCUMENTS LIST

JUNE 2013

Information Technology (IT) Security Applicable Documents List
JUNE 2013

NASA Policy Directives (NPD) and NASA Procedural Requirements (NPR)		
Document	**Subject**	**Effective Date**
NPR 1382.1	NASA Privacy Procedural Requirements	August 10, 2007
NPD 1382.17H	NASA Privacy Policy	June 24, 2009
NPD 1440.6H	NASA Records Management	March 24, 2008
NPR 1441.1D	NASA Records Retention Schedules (w/Change 5, 6/29/09)	February 24, 2003
NPD 2540.1G	Personal Use of Government Office Equipment Including Information Technology	June 08, 2010
NPD 2800.1B	Managing Information Technology	March 21, 2008
NPR 2800.1B	Managing Information Technology	March 20, 2009
NPD 2810.1D	NASA Information Security Policy	May 9, 2009
NPR 2810.1A	Security of Information Technology w/ Change 1, May 19, 2011)	May 16, 2006
NPD 2830.1A	NASA Enterprise Architecture	November 2, 2011
NPR 2830.1	NASA Enterprise Architecture Procedures	February 9, 2006
NPR 7120.7	NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements	November 3, 2008
NPR 2841.1	Identity, Credential, and Access Management	January 6, 2011

NASA Interim Directive		
Document	**Subject**	**Effective Date**
NM2810-64	NASA Interim Directive: Information Technology Security and Efficiency Requirements	May 22, 2008

NASA Interim Technical Requirements (NITR)		
Document	**Subject**	**Effective Date**
NITR 2800_2	Email Services and Email Forwarding	September 18, 2009
NITR 2800_1	NASA Information Technology Waiver Requirements and Procedures	August 13, 2009
NITR 2830-1B	Networks in NASA Internet Protocol (IP) Space or NASA Physical Space	February 12, 2009
NITR 1382_2	NASA Rules and Consequences to Safeguarding PII, with Change 1, dated 02/04/2008	January 28, 2008

SOPs (ITS-SOP) and Handbooks (ITS-HBK)		
Document	**Subject**	**Effective Date**
ITS-HBK-2810.0001-A	Format and Procedures for an IT Security Handbook	March 29, 2011
ITS-HBK-2810.0002-A	Roles and Responsibilities Crosswalk	May 2, 2013
ITS-HBK-2810.02-01	Security Assessment and Authorization	May 6, 2011
ITS-HBK-2810.02-02	Security Assessment and Authorization: FIPS 199 Moderate & High Systems	October 24, 2012
ITS-HBK-2810.02-03	Security Assessment and Authorization: FIPS 199 Low Systems	October 24, 2012
ITS-HBK-2810.02-04	Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments	October 24, 2012
ITS-HBK-2810.02-05	Security Assessment and Authorization: External Information Systems	October 24, 2012
ITS-HBK-2810.02-06	Security Assessment and Authorization: Extending and Information Systems Authorization to Operate Process and Templates	October 24, 2012

SOPs (ITS-SOP) and Handbooks (ITS-HBK)		
Document	**Subject**	**Effective Date**
ITS-HBK-2810.02-07	Security Assessment and Authorization: Information System Security Plan Numbering Schema	February 27, 2012
ITS-HBK-2810.02-08	Security Assessment and Authorization: Plan of Action and Milestones (POA&M)	August 21, 2012
ITS-HBK-2810.03-01	Planning	May 6, 2011
ITS-HBK-2810.03-02	Planning: Information System Security Plan Template, Requirements, Guidance and Examples	February 9, 2011
ITS-HBK-2810.04-01-A	Risk Assessment: Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching & Organizationally Defined Values	October 12, 2012
ITS-HBK-2810.04-02-A	Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement	April 30, 2013
ITS-HBK-2810.04-03	Risk Assessment: Web Application Security Program	April 30, 2013
ITS-HBK-2810.05-01	Systems and Service Acquisition	November 21, 2011
ITS-HBK-2810.06-01	Awareness and Training	May 6, 2011
ITS-HBK-2810.07-01	Configuration Management	May 6, 2011
ITS-HBK-2810.08-01	Contingency Planning	May 6, 2011
ITS-HBK-2810.08-02	Contingency Planning: Guidance and Templates for Plan Development, Maintenance and Test	February 11, 2011
ITS-HBK-2810.09-01	Incident Response and Management	May 6, 2011
ITS-HBK-2810.09-02	Incident Response and Management: NASA Information Security Incident Management	August 24, 2011
ITS-HBK-2810.09-03	Incident Response and Management: Targeted Collection of Electronic Data	August 24, 2011

SOPs (ITS-SOP) and Handbooks (ITS-HBK)		
Document	**Subject**	**Effective Date**
ITS-HBK-2810.10-01	Maintenance	May 6, 2011
ITS-HBK-2810.11-01-A	Media Protection	July 13, 2012
ITS-HBK-2810.11-02	Media Protection: Digital Media Sanitization	July 13, 2012
ITS-HBK-2810.12-01	Physical and Environmental Protection	May 6, 2011
ITS-HBK-2810.13-01	Personnel Security	May 6, 2011
ITS-HBK-2810.14-01	System and Information Integrity	May 6, 2011
ITS-HBK-2810.15-01-A	Access Control	September 4, 2012
ITS-HBK-2810.15-02-A	Access Control: Elevated Privileges (EP)	September 20, 2012
ITS-HBK-2810.16-01	Audit and Accountability	May 6, 2011
ITS-HBK-2810.17-01	Identification and Authentication	May 6, 2011
ITS-HBK-2810.18-01	System and Communications Protection	May 6, 2011

Standards		
Document	**Subject**	**Effective Date**
EA-STD 0001.0	Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorization Infrastructure	August 1, 2008
EA-SOP 0003.0	Procedures for Submitting a NASA Agency Forest (NAF) Deviation Request and Transition Plan	August 1, 2008
EA-SOP 0004.0	Procedures for Submitting an Application Integration Deviation Request and Transition Plan	August 1, 2008
NASA-STD-2804-O	Minimum Interoperability Software Suite	August 9, 2011
NASA-STD-2805-O	Minimum Hardware Configurations	August 9, 2011

Memoranda				
From	**To**	**Subject**	**Effective Date**	**Posted Date**
Associate Deputy Administrator	All NASA Employees	Breach of Personally Identifiable Information (PII) [Laptop DAR/Encryption]	11/13/12	11/13/12
Charles F. Bolden, Jr., NASA Administrator	All NASA Employees	Protection of Sensitive Agency Information	4/3/2012	4/3/2012
Chief Information Officer	All NASA Civil Service and Contractor Employees	Policy for Use of Removable Media, Such as USB Thumb Drives	11/21/2008	11/21/2008

Within 30 days after contract effective date, the Contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer for approval.