nsacyber.github.io

NSA Cybersecurity publications

This page lists NSA Cybersecurity publications.

- Current NSA Cybersecurity publications can be found under the **Resources for Cybersecurity Professionals** section at https://www.nsa.gov/what-we-do/cybersecurity/
- Archived NSA Information Assurance and Information Assurance Directorate publications can be found at https://apps.nsa.gov/iaarchive/library (formerly https://www.iad.gov)

A zip file containing publications from both pages can be downloaded from https://github.com/nsacyber/nsacyber.github.io/releases/latest

* notes when authorization is required to access a publication.

Table of Contents

Title	Location	Date	Size
Patch Remote Desktop Services On Legacy Versions of Windows (more…)	Current	Jun 2019	416KB
Limiting ptrace on Production Linux Systems (more…)	Current	May 2019	128KB

Title	Location	Date	Size
Update Earlier Versions of Solaris to 11.4 (more…)	Current	Mar 2019	422KB
Updated Guidance For Vulnerabilities Affecting Modern Processors (more…)	Current	Jan 2019	322KB
NSA/CSS Technical Cyber Threat Framework v2 (more…)	Current	Nov 2018	2,150KB
2018 Cybersecurity Highlights (more…)	Current	Oct 2018	416KB
Identity Theft Threat and Mitigations (more…)	Archive	Sep 2018	316KB
Best Practices for Keeping Your Home Network Secure (more…)	Archive	Sep 2018	291KB
A Guide to Border Gateway Protocol (BGP) Best Practices (more…)	Archive	Sep 2018	222KB
Best Practices for Keeping Your Home Network Secure (more…)	Current	Sep 2018	577KB
A Guide to Border Gateway Protocol (BGP) Best Practices (more…)	Current	Sep 2018	1,117KB
Identity Theft Threat and Mitigations (more…)	Current	Sep 2018	789KB

Title	Location	Date	Size
Cloud Security Basics (more…)	Archive	Aug 2018	215KB
Cloud Security Basics (more…)	Current	Aug 2018	628KB
Blocking Unnecessary Advertising Web Content (more…)	Archive	Jul 2018	203KB
Blocking Unnecessary Advertising Web Content (more…)	Current	Jul 2018	505KB
WPA3 will Enhance Wi-Fi Security (more…)	Archive	Jun 2018	441KB
Mobile Device Best Practices When Traveling OCONUS (more…)	Archive	Jun 2018	234KB
How to fulfill the Requirement to Upgrade Symantec Proxy CAS (more…)*	Current	Jun 2018	
WordPress Plugin WP Symposium Remote Code Execution CVE-2014-10021 (more…)*	Current	Jun 2018	
WPA3 Will Enhance Wi-Fi Security (more…)	Current	Jun 2018	709KB
Steps to Secure Web Browsing (more…)	Archive	May 2018	135KB

Title	Location	Date	Size
Mobile Device Best Practices When Traveling OCONUS (more…)	Current	May 2018	319KB
Steps to Secure Web Browsing (more…)	Current	May 2018	461KB
Drupal Unauthenticated Remote Code Execution Vulnerability CVE-2018-7600 (more…)	Archive	Apr 2018	119KB
Multiple Critical Vulnerabilities Identified in Cisco Smart Install (more…)	Archive	Apr 2018	493KB
Windows 10 for Enterprises Security Benefits of Timely Adoption (more…)	Archive	Apr 2018	280KB
Seven Steps to Effectively Defend Industrial Control Systems (more…)	Archive	Apr 2018	797KB
Windows 10 for Enterprises Security Benefits of Timely Adoption (more…)	Current	Apr 2018	379KB
Multiple Critical Vulnerabilities Identified in CISCO Smart Install (more…)	Current	Apr 2018	451KB
Drupal Unauthenticated Remote Code Execution Vulnerability (more…)	Current	Apr 2018	289KB
UNFETTER (more…)	Archive	Mar 2018	730KB

Title	Location	Date	Size
NSA/CSS Technical Cyber Threat Framework v1 (more…)	Archive	Mar 2018	1,275KB
NSAs Top Ten Cybersecurity Mitigation Strategies (more…)	Archive	Mar 2018	194KB
NCTOC Top 5 Security Operations Center (SOC) Principles (more…)	Current	Mar 2018	126KB
UNFETTER (more…)	Current	Mar 2018	494KB
Top 10 Mitigation Strategies (more…)	Current	Mar 2018	348KB
UEFI Lockdown Quick Guidance (more…)	Current	Mar 2018	416KB
UEFI Advantages Over Legacy Mode (more…)	Current	Mar 2018	336KB
Unified Extensible Firmware Interface (UEFI) Advantages (more…)	Archive	Feb 2018	352KB
Cisco Updates Critical Remote Code Execution Vulnerability Advisory for ASA (more…)	Archive	Feb 2018	197KB
CISCO Updates Critical Remote Code Execution Vulnerability for ASA (more…)	Current	Feb 2018	283KB

Title	Location	Date	Size
Inspection and Sanitization Guidance for Exchangeable Image Format (EXIF) (more…)	Archive	Feb 2018	933KB
Inspection and Sanitization Guidance for the DOD Electronic Biometric Transmission Specifications (EBTS) File Format (more…)	Archive	Feb 2018	1,672KB
Analysis of Optical Character Recognition (OCR) Techniques for Security Marking Detection (more…)	Archive	Feb 2018	979KB
Security Guidance for JSON and JSON Schema (more…)	Archive	Feb 2018	880KB
Inspection and Sanitization Guidance for PNG (more…)	Archive	Feb 2018	931KB
Inspection and Sanitization Guidance for MPEG-2 (more…)	Archive	Feb 2018	2,887KB
UEFI Lockdown Quick Guidance (more…)	Archive	Jan 2018	464KB
Verification, Inspection, and Sanitization Report Specification (more…)	Archive	Jan 2018	682KB
Unicode Security Risks (more…)	Archive	Jan 2018	715KB
Inspection and Sanitization Guidance for National Imagery Transmission Format (NITF) (more…)	Archive	Jan 2018	1,116KB

Title	Location	Date	Size
DotNetNuke Remote Code Execution Vulnerability CVE-2017-9822 (more…)	Archive	Jan 2018	339KB
Vulnerabilities Affecting Modern Processors (more…)	Archive	Jan 2018	288KB
Vulnerabilities Affecting Modern Processors (more…)	Current	Jan 2018	512KB
DotNetNuke Remote Code Execution Vulnerability (more…)	Current	Jan 2018	353KB
Securing Kernel Modules on Linux Operating Systems (more…)	Archive	Dec 2017	238KB
Bro NSM Hunting Tips (more…)	Archive	Dec 2017	1,141KB
RSA SecurID Token Authentication Agent Vulnerabilities (more…)	Archive	Dec 2017	226KB
RSA SecureID Token Authentication Agent Vulnerabilities (more…)	Current	Dec 2017	392KB
Inspection and Sanitization Guidance for TIFF File Formats (more…)	Archive	Nov 2017	1,334KB
RSA Key Generation Vulnerability Affecting Trusted Platform (more…)	Archive	Oct 2017	271KB

Title	Location	Date	Size
Mitigations for Key Reinstallation Attacks Against Wi-Fi Protected Access II (WPA2) (more…)	Archive	Oct 2017	101KB
Mitigations for Key Reinstallation Attacks Against WI-FI Protected Access II (WPA2) (more…)	Current	Oct 2017	338KB
RSA Key Generation Vulnerability Affecting Trusted Platform Modules (more…)	Current	Oct 2017	342KB
Cisco Smart Install Protocol Misuse (more…)	Archive	Aug 2017	270KB
CISCO Smart Install Protocol Misuse (more…)	Current	Aug 2017	357KB
Security Guidance for the Use of JSON and JSON Schemas (more…)	Archive	Jul 2017	1,041KB
Juniper Network Announces Multiple Critical Vulnerabilities (more…)	Archive	Jul 2017	190KB
UEFI Defensive Practices Guidance (more…)	Current	Jul 2017	1,790KB
Cisco Simple Network Management Protocol Buffer Overflow Vulnerabilities (more…)	Archive	Jun 2017	119KB
Frank B Rowlett Award for Organizational Excellence (more…)	Archive	Jun 2017	2,425KB

Title	Location	Date	Size
Devices with Intel Atom C2000 Series Processors (more…)	Archive	Jun 2017	159KB
National Security Cyber Assistance Program Cyber Incident Response Assistance Accreditation Instruction Manual (more…)	Archive	Jun 2017	1,461KB
National Security Cyber Assistance Program Accredited Companies' Contact Information (more…)	Archive	Jun 2017	86KB
Advanced Concepts - Information Assurance Solutions at the Speed of Technology (more…)	Archive	Jun 2017	457KB
Network Security Devices Utilizing Vulnerable Weak Signature Algorithms in TLS (more…)	Archive	Jun 2017	505KB
Network Security Devices Utilizing Vulnerable Weak Signature Algorithms in TLS (more…)	Current	Jun 2017	527KB
Whitelisting Windows IIS and WebDAV Traffic (more…)	Archive	May 2017	2,003KB
Mitigations for WannaCrypt-WannaCry Ransomware (more…)	Archive	May 2017	185KB
CVE-2017-5689: Intel AMT, Intel ISM Privilege Escalation (more…)	Archive	May 2017	191KB
Faulty Intel Atom C2000 Processor (more…)	Archive	May 2017	493KB

Title	Location	Date	Size
Privileged Access Management (more…)	Archive	Apr 2017	257KB
Apply Kernel Protection on Windows 7 and Windows 7 SP1 - Updated (more…)	Archive	Apr 2017	115KB
Establishing NSA's position on the use of Trusted Platform Modules in National Security Systems (more…)	Archive	Apr 2017	185KB
Least Privilege (more…)	Archive	Apr 2017	960KB
March 2017 Patch Tuesday (more…)	Archive	Mar 2017	179KB
Removal of Server Message Block 1.0 (more…)	Archive	Mar 2017	230KB
Overview of Software Defined Networking Risks (more…)	Archive	Feb 2017	2,587KB
Commercial Solutions for Classified Tri-fold (more…)	Archive	Jan 2017	111KB
Commercial Solutions for Classified Brochure (more…)	Archive	Jan 2017	24,218KB
Reducing the Risk of Simple Network Management Protocol Abuse (more…)	Archive	Jan 2017	540KB

Title	Location	Date	Size
National Information Assurance Partnership 2016 Report (more…)	Archive	Jan 2017	545KB
Community Gold Standard Brochure (more…)	Archive	Jan 2017	461KB
Reducing the Risk of Vulnerabilities in Unix/Linux-Based Operating Systems (more…)	Archive	Jan 2017	222KB
PowerShell: Security Risks and Defenses (more…)	Archive	Dec 2016	277KB
Windows 10 for Enterprises (more…)	Archive	Dec 2016	463KB
Long-lived Hashes for Active Directory SmartCard Required Accounts (more…)	Archive	Nov 2016	392KB
Eliminating Control Flow Exploitation (more…)	Archive	Nov 2016	1,558KB
Voice and Video over IP (more…)	Archive	Nov 2016	939KB
Top Ten IA Mitigations (more…)	Archive	Nov 2016	1,544KB
Overcoming Barriers to Adopting Top 10 IA Mitigations (more…)	Archive	Nov 2016	1,871KB

Title	Location	Date	Size
Securely Configuring Adobe Acrobat (more…)	Archive	Nov 2016	1,120KB
Mitigating Insider Threats (more…)	Archive	Nov 2016	931KB
Comply to Connect (more…)	Archive	Nov 2016	1,106KB
Application Whitelisting Best Practices (more…)	Archive	Nov 2016	1,394KB
Algorithms to Support the Evolution of Information Assurance Needs (more…)	Archive	Nov 2016	119KB
Application Isolation Containment (more…)	Archive	Nov 2016	907KB
Building the Cyber Workforce Pipeline: Preparing for Today, Tomorrow, and the Day After Tomorrow (more…)	Archive	Nov 2016	1,589KB
The NSA Codebreaker Challenge (more…)	Archive	Nov 2016	817KB
Training and Certification:Impacting NSA's Mission (more…)	Archive	Nov 2016	1,694KB
Joint COMSEC Monitoring Activity Findings and Trends (more…)	Archive	Nov 2016	1,093KB

Title	Location	Date	Size
Compliance Training for Technical Professionals: A Case Study (more…)	Archive	Nov 2016	2,243KB
Third Party Services Your Risk Picture Just Got a Lot More Complex (more…)	Archive	Nov 2016	864KB
Making Mitigations Matter Measuring Host Mitigation State (more…)	Archive	Nov 2016	613KB
Defending Against the Malicious Use of Admin Tools: PowerShell (more…)	Archive	Nov 2016	850KB
Blocking Macros from Internet Originated Microsoft Office Files (more…)	Archive	Nov 2016	189KB
Hardening Authentication Update (more…)	Archive	Nov 2016	319KB
Manageable Network Plan Teaser Update (more…)	Archive	Nov 2016	301KB
Assess the Mess (more…)	Archive	Nov 2016	3,847KB
Linux Kernel Privilege Escalation Vulnerability CVE-2016-5195 (more…)	Archive	Oct 2016	275KB
Security Configuration Guide for Browser Updates (more…)	Archive	Oct 2016	721KB

Title	Location	Date	Size
Best Practices for Keeping Your Home Network Secure (Update) (more…)	Archive	Sep 2016	341KB
Recommendations to Mitigate IKEv1 Vulnerability in Cisco Network Devices (more…)	Archive	Sep 2016	216KB
Outdated Network Devices and Unsecure Protocols and Services Expose Network Infrastructure to Compromise (more…)	Archive	Sep 2016	893KB
Vulnerabilities in Cisco Adaptive Security Appliances Identified in Open-Source – Version 1 (more…)	Archive	Aug 2016	196KB
Bluetooth for Unclassified Use: A Risk Discussion for IT Decision Makers (more…)	Archive	Aug 2016	348KB
Bluetooth for Unclassified Use: Guidelines for Users (more…)	Archive	Aug 2016	313KB
Bluetooth for Unclassified Use: Guidelines for Developers (more…)	Archive	Aug 2016	340KB
Take Advantage of Software Improvement (more…)	Archive	Aug 2016	329KB
Implementing a Secure Administrator Workstation Using Device Guard (more…)	Archive	Jul 2016	957KB
Outdated Software and Protocols Updated (more…)	Archive	Jul 2016	448KB

Title	Location	Date	Size
Recommendations to Mitigate Unauthorized Cisco ROMMON Access and Validate Boot ROMs (more…)	Archive	Jul 2016	160KB
Filter Sidecar Protocol (FSP) Specification (more…)	Archive	Jul 2016	822KB
Network Mitigations Package-Infrastructure (more…)	Archive	Jun 2016	1,010KB
Perform Out-of-Band Network Management (more…)	Archive	Jun 2016	493KB
Validate Integrity of Hardware and Software (more…)	Archive	Jun 2016	621KB
Harden Network Devices (more…)	Archive	Jun 2016	459KB
Secure Access to Infrastructure Devices (more…)	Archive	Jun 2016	496KB
National Security Cyber Assistance Program Vulnerability Assessment Accreditation Scoresheet 1.0 (more…)	Archive	Jun 2016	56KB
Protecting Virtual Private Network Traffic 2016 (more…)	Archive	Jun 2016	416KB
Guidelines for ConfigurationPatch Management in Industrial Control Systems (more…)	Archive	May 2016	1,663KB

Title	Location	Date	Size
ImageMagick Remote Code Execution Vulnerability CVE-2016-3714 (more…)	Archive	May 2016	277KB
Information Assurance Advisory Information Sheet (more…)	Archive	May 2016	369KB
Apple Quicktime Reaches End-of-Life for Windows Factsheet (more…)	Archive	May 2016	194KB
National Security Cyber Assistance Program Cyber Incident Response Assistance Accreditation Instruction Manual 3.2 (more…)	Archive	May 2016	2,527KB
National Security Cyber Assistance Program VAS Accreditation Instruction Manual (more…)	Archive	May 2016	1,343KB
Wireless Intrusion Detection System Technical Brief (more…)	Archive	Apr 2016	307KB
Ransomware - Locky (more…)	Archive	Apr 2016	418KB
Guidelines for Application Whitelisting Industrial Control Systems (more…)	Archive	Apr 2016	1,065KB
Joint Information Environment (more…)	Archive	Mar 2016	600KB
Information Assurance Top 9 Architectural Tenets (more…)	Archive	Mar 2016	308KB

Title	Location	Date	Size
Trusted Engineering Solutions (more…)	Archive	Mar 2016	739KB
Security Highlights of Windows 10 (more…)	Archive	Feb 2016	664KB
Network Device Integrity -NDI- Methodology (more…)	Archive	Feb 2016	231KB
Network Device Integrity on Cisco IOS Devices (more…)	Archive	Feb 2016	361KB
IAD's Top 10 Information Assurance Mitigation Strategies (more…)	Archive	Feb 2016	463KB
Position Zero: Integrity Checking Windows-Based ICS/SCADA Systems (more…)	Archive	Feb 2016	3,563KB
2016 IAD's Top Challenges and Efforts (more…)	Archive	Jan 2016	659KB
Journal of Information Warfare, Vol. 14 Issue 2 (more…)	Archive	Jan 2016	2,868KB
Commercial National Security Algorithm Suite and Quantum Computing FAQ (more…)	Archive	Jan 2016	253KB
IAD Top Ten Mitigations Questions and Answers (more…)	Archive	Jan 2016	504KB

Title	Location	Date	Size
Commercial National Security Algorithm Suite Factsheet (more…)	Archive	Dec 2015	344KB
Seven Steps to Effectively Defend Industrial Control Systems (more…)	Archive	Dec 2015	1,383KB
Recommendations for Configuring Adobe Acrobat Reader DC in a Windows Environment (more…)	Archive	Dec 2015	506KB
Manageable Network Plan Guide (more…)	Archive	Dec 2015	5,533KB
IAD's Top 10 Information Assurance Mitigation Strategies (more…)	Archive	Nov 2015	331KB
IAD Best Practices for Securing Wireless Devices and Networks in National Security Systems (more…)	Archive	Oct 2015	989KB
Community Gold Standard 1.1.1 files (more…)	Archive	Oct 2015	25,692KB
Securing Assets Within a Closed Industrial Control System Network (more…)	Archive	Oct 2015	1,354KB
Securely Managing Industrial Control System Networks (more…)	Archive	Oct 2015	198KB
Cyber Defense Exercise Winners (more…)	Archive	Sep 2015	141KB

Title	Location	Date	Size
Microsoft's Enhanced Mitigation Experience Toolkit: A Rationale for Enabling Modern Anti-Exploritation Mitigations in Windows (more…)	Archive	Sep 2015	1,275KB
National Security Cyber Assistance Program Frequently Asked Questions (more…)	Archive	Sep 2015	833KB
Scripting for Bash Vulnerability/Shellshock (more…)	Archive	Sep 2015	665KB
Microsoft's Enhanced Mitigation Experience Toolkit Guide (more…)	Archive	Sep 2015	1,488KB
Host Mitigation Package (more…)	Archive	Sep 2015	1,288KB
Security Highlights of Windows 7 (more…)	Archive	Sep 2015	412KB
Application Whitelisting using Software Restriction Policies (more…)	Archive	Sep 2015	385KB
Security Content Automation Protocol Content for Apple iOS 5 Security Configuration Recommendations (more…)	Archive	Sep 2015	29KB
Recommendations for Configuring Adobe Acrobat Reader XI in a Windows Environment (more…)	Archive	Sep 2015	330KB
Reducing the Effectiveness of Pass-the-Hash (more…)	Archive	Sep 2015	350KB

Title	Location	Date	Size
Spotting the Adversary with Windows Event Log Monitoring (more…)	Archive	Sep 2015	871KB
Defense in Depth (more…)	Archive	Sep 2015	670KB
NSA Methodology for Adversary Obstruction (more…)	Archive	Aug 2015	741KB
Adobe ColdFusion Guidance (more…)	Archive	Jul 2015	627KB
Virtual Private Network Registration Form (more…)	Archive	Jun 2015	1,017KB
Campus Wireless Local Area Network Registration Form (more…)	Archive	Jun 2015	1,017KB
2014 Supplemental Guide to the National Manager's Letter (more…)	Archive	May 2015	687KB
Frank B. Rowlett Awards Program (more…)	Archive	Mar 2015	56KB
Apply for Cyber Incident Response Assistance Accreditation Using the National Security Cyber Assistance Program Accreditation Portal (more…)	Archive	Mar 2015	234KB
2015 IAD's Top Technology Challenges (more…)	Archive	Feb 2015	266KB

Title	Location	Date	Size
Inspection and Sanitization Guidance for the Graphics Interchange Format (GIF) (more…)	Archive	Feb 2015	997KB
Accreditation Portal User's Guide (more…)	Archive	Jan 2015	4,595KB
Defensive Best Practices for Destructive Malware (more…)	Archive	Jan 2015	926KB
Cyber Incident Response Assistance Accreditation (more…)	Archive	Dec 2014	9,086KB
Bash Bug (ShellShock) (more…)	Archive	Oct 2014	337KB
Scripting for Bash Vulnerability/Shellshock (more…)	Archive	Oct 2014	665KB
Microsoft's Enhanced Mitigation Experience Toolkit Guide (more…)	Archive	Oct 2014	1,488KB
Wireless Vulnerabilities Article (more…)	Archive	Oct 2014	28KB
Understanding the Enhanced Mitigation Experience Toolkit Frequently Asked Questions (more…)	Archive	Oct 2014	396KB
Microsoft's Enhanced Mitigation Experience Toolkit: A Rationale for Enabling Modern Anti-Exploritation Mitigations in Windows (more…)	Archive	Oct 2014	1,275KB

Title	Location	Date	Size
National Security Cyber Assistance Program Brochure (more…)	Archive	Sep 2014	3,370KB
How National Security Cyber Assistance Program Benefits Service Providers and National Security System Owners (more…)	Archive	Sep 2014	108KB
Critical Focus Areas of Cyber Incident Response Assistance (more…)	Archive	Sep 2014	846KB
Cisco Adaptive Security Appliance Out-of-the-Box Security Configuration Guide (more…)	Archive	Sep 2014	310KB
Inspection and Sanitization Guidance for Simple Mail Transfer Protocol (SMTP), Internet Message Format (IMF), and Multipurpose Internet Mail Extensions (MIME) (more…)	Archive	Sep 2014	1,105KB
Email Filtering Best Practices Guide Version 1.0 (more…)	Archive	Sep 2014	418KB
Application Whitelisting Using Microsoft AppLocker (more…)	Archive	Aug 2014	1,748KB
Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network (more…)	Archive	Jul 2014	2,988KB
2014 IAD's Top Technology Challenges (more…)	Archive	Jul 2014	173KB
Information Assurance Guidance for Microsoft Windows XP End of Life (more…)	Archive	Jul 2014	417KB

Title	Location	Date	Size
Community Gold Standard 2.0 (more…)	Archive	Jun 2014	1,558KB
Identity Theft Threat and Mitigations (more…)	Archive	May 2014	2,374KB
Factsheet: Mitigations for OpenSSL TLS/DTLS Heartbeat Extension Vulnerability (more…)	Archive	May 2014	236KB
Best Practices for Keeping Your Home Network Secure (more…)	Archive	May 2014	1,894KB
Journal of Information Warfare, Vol. 13 Issue 2 (more…)	Archive	Apr 2014	3,484KB
Supplemental Guide to the National Manager's Letter 2014 (more…)	Archive	Mar 2014	773KB
Supplemental Guide to the National Manager's Letter 2015 (more…)	Archive	Mar 2014	1,862KB
Random Number Generators: Introduction for Operating System Developers (more…)	Archive	Mar 2014	644KB
Random Number Generators: Introduction for Application Developers (more…)	Archive	Mar 2014	582KB
Inspection and Sanitization Guidance for the Wavelet Scalar Quantization (WSQ) Biometric Image Format (more…)	Archive	Jan 2014	610KB

Title	Location	Date	Size
Spotting the Adversary with Windows Event Log Monitoring (more…)	Archive	Dec 2013	871KB
Host Mitigation Package (more…)	Archive	Dec 2013	1,288KB
Reducing the Effectiveness of Pass-the-Hash (more…)	Archive	Nov 2013	350KB
Web Domain Name System Reputation (more…)	Archive	Oct 2013	712KB
Segregate Networks and Functions (more…)	Archive	Oct 2013	414KB
Secure Host Baseline (more…)	Archive	Oct 2013	491KB
Limit Workstation-to-Workstation Communication (more…)	Archive	Oct 2013	502KB
Host Intrusion Prevention Systems (more…)	Archive	Oct 2013	618KB
Control Administrative Privileges (more…)	Archive	Oct 2013	655KB
Cloud Security Considerations (more…)	Archive	Oct 2013	1,046KB

Title	Location	Date	Size
Application Whitelisting (more…)	Archive	Oct 2013	597KB
Anti-Virus File Reputation Services (more…)	Archive	Oct 2013	528KB
Anti-Exploitation Features (more…)	Archive	Oct 2013	520KB
Recommendations for Configuring Adobe Acrobat Reader XI in a Windows Environment (more…)	Archive	Jul 2013	330KB
Building Web Applications Security Recommendations for Developers (more…)	Archive	Apr 2013	534KB
Host Based Security System Application Whitelisting Technical Implementation Guide (more…)	Archive	Mar 2013	7,020KB
Inspection and Sanitization Guidance for HyperText Transport Protocol (HTTP) (more…)	Archive	Nov 2012	1,004KB
Inspection and Sanitization Guidance for JPEG 2000 (more…)	Archive	Nov 2012	743KB
Deploying Signed BIOSes to Enterprise Client Systems (more…)	Archive	Nov 2012	359KB
Inspection and Sanitization Guidance for JPEG File Interchange Format (more…)	Archive	Nov 2012	639KB

Title	Location	Date	Size
JavaScript Security Risks (more…)	Archive	Nov 2012	1,021KB
Configuring Windows To Go as a Mobile Desktop Solution (more…)	Archive	Nov 2012	420KB
Deploying and Securing Google Chrome in a Windows Enterprise (more…)	Archive	Oct 2012	725KB
Community Gold Standard Brochure (more…)	Archive	Oct 2012	4,396KB
Securing Data and Handling Spillage Events (more…)	Archive	Oct 2012	673KB
Hardening Authentication (more…)	Archive	Sep 2012	708KB
Mobile Device Management: Capability Gaps for High-Security Use Cases (more…)	Archive	Aug 2012	734KB
Mobile Device Management: A Risk Discussion for IT Decision Makers (more…)	Archive	Aug 2012	734KB
Defending Against Compromised Certificates (more…)	Archive	Jul 2012	306KB
Guidelines for Regular Expressions in XML Schemas (more…)	Archive	Jun 2012	964KB

Title	Location	Date	Size
XSLT 1.0 Recommendations for Making XSLT Programs Behave as Expected (more…)	Archive	Jun 2012	684KB
Using Schematron for Cross Domain Security Policy Enforcement (more…)	Archive	Jun 2012	623KB
Basic XML Security Considerations (more…)	Archive	Jun 2012	278KB
Frank B. Rowlett Award for Individual Excellence Nomination Form (more…)	Archive	May 2012	2,425KB
Security Content Automation Protocol Content for Apple iOS 5 Security Configuration Recommendations (more…)	Archive	May 2012	29KB
New Smartphones and the Risk Picture (more…)	Archive	Apr 2012	982KB
Security Configuration Recommendations for Apple iOS 5 Devices (more…)	Archive	Mar 2012	235KB
Inspection and Sanitization Guidance for HyperText Markup Language (HTML) (more…)	Archive	Mar 2012	1,559KB
Inspection and Sanitization Guidance for Cascading Style Sheets (more…)	Archive	Mar 2012	937KB
Inspection and Sanitization Guidance for Bitmap File Format (more…)	Archive	Mar 2012	654KB

Title	Location	Date	Size
Inspection and Sanitization Guidance for Waveform Audio File Format (more…)	Archive	Mar 2012	1,397KB
Inspection and Sanitization Guidance for Rich Text Format (RTF) (more…)	Archive	Mar 2012	1,068KB
Mitigation Monday #3: Defense against Malware on Removable Media (more…)	Archive	Mar 2012	692KB
Security Tips for Personally Managed Apple iPhones and iPads (more…)	Archive	Jan 2012	255KB
Redaction of Portable Document Format Files Using Adobe Acrobat Professional X (more…)	Archive	Nov 2011	809KB
Hardening Deployed Web Applications (more…)	Archive	Sep 2011	6,311KB
Protect Against Cross Site Scripting Attacks (more…)	Archive	Sep 2011	349KB
Guide to the Secure Configuration of Red Hat Enterprise Linux 5 (more…)	Archive	Aug 2011	867KB
Enforcing No Internet or E-mail from Privileged Accounts (more…)	Archive	Aug 2011	539KB
Host Protection Technology Study (more…)	Archive	Jun 2011	3,398KB

Title	Location	Date	Size
Security Guidance for the use of XML Schema 1.0/1.1 and RELAX NG (more…)	Archive	May 2011	1,146KB
Inspection and Sanitization Guidance for Portable Document Format (more…)	Archive	May 2011	2,141KB
Guidelines for Implementation of REST (more…)	Archive	Mar 2011	708KB
BIND 9 Domain Name System Security (more…)	Archive	Feb 2011	225KB
Unified Communications Technical Primer (more…)	Archive	Jan 2011	433KB
Security Highlights of Windows 7 (more…)	Archive	Oct 2010	412KB
Securing Lotus Sametime (more…)	Archive	Sep 2010	494KB
A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (more…)	Archive	Aug 2010	936KB
Inspection and Sanitization Guidance for Microsoft Office 2003 (more…)	Archive	Aug 2010	1,070KB
Cisco Unified Presence Server (more…)	Archive	Aug 2010	535KB

Title	Location	Date	Size
Application Whitelisting using Software Restriction Policies (more…)	Archive	Aug 2010	385KB
Application Whitelisting (more…)	Archive	Aug 2010	543KB
Inspection and Sanitization Guidance for Microsoft Office 2007 and Office Open XML (OOXML) (more…)	Archive	Jun 2010	1,222KB
Activating Authentication and Encryption for Cisco Unified Communications Manager Express 7.0/4.3 (more…)	Archive	Apr 2010	551KB
Mathematical routines for the National Institute of Standards and Technology prime elliptic curves (more…)	Archive	Apr 2010	205KB
Host and Network Integrity through Trusted Computing (more…)	Archive	Apr 2010	560KB
Defense in Depth (more…)	Archive	Mar 2010	670KB
Hardening Tips for Mac OS X 10.6 Snow Leopard (more…)	Archive	Mar 2010	485KB
Suite B Implementer’s Guide to Federal Information Processing Standard 186-3 (more…)	Archive	Feb 2010	177KB

Publications

Patch Remote Desktop Services On Legacy Versions of Windows

- Abstract:
- Date: 06/01/2019
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep_20190604.pdf?ver=2019-06-04-123329-617
- Category: Advisory
- SHA256: 3B065C245CEB7B5B35C44EE82223434FF5DED69CAE64CA0AB2B8FF2B937FA6F0
- Size: 416KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Limiting ptrace on Production Linux Systems

- Abstract:
- Date: 05/01/2019
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-limiting-ptrace-on-production-linux-systems.pdf?ver=2019-05-16-151825-133
- Category: Info Sheet
- SHA256: C15D35F9F1F6A9F939028C41C2D5E5F6FEAAF49DD9ADC7B4A34A401C833F156C
- Size: 128KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Update Earlier Versions of Solaris to 11.4

- Abstract:
- Date: 03/01/2019
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-upgrade-solaris11-4.pdf?ver=2019-03-14-093217-840
- Category: Advisory
- SHA256: C337EFFFBA49CF2F7671517D6253580B6EBF74098EF333FC8271C978D19ABDF6
- Size: 422KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Updated Guidance For Vulnerabilities Affecting Modern Processors

- Abstract:
- Date: 01/01/2019
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/CSA_Updated_Guidance_For_Vulnerabilities_Affecting_Modern_Processors_20190130.pdf?ver=2019-01-30-142631-553
- Category: Advisory
- SHA256: F2F827B4361DC505870EA5AC8F1585E84F30347875D870B738AFCAD16A68351A
- Size: 322KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

NSA/CSS Technical Cyber Threat Framework v2

- Abstract:
- Date: 11/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf
- Category: Tech Report
- SHA256: F86E222CE7E2C4ADB630CA8FB460533098ECDE805AB3FF551BEBC5C0DB702F57
- Size: 2,150KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

2018 Cybersecurity Highlights

- Abstract:
- Date: 10/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-cybersecurity-highlights-2018.pdf
- Category: Info Sheet
- SHA256: 0A083DB89E6F03637A9E1DEF61C505EDB90C5C42BF172AD6AC2C8AD90C5C313E
- Size: 416KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Identity Theft Threat and Mitigations

- Abstract: Identity theft is a crime that involves using another person's personal information to take malicious actions, such as conducting fraud or stealing funds. The information provided in this document is designed to help individuals protect themselves against identity theft and mitigate the risk.
- Date: 09/26/2018
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/faq/identity-theft-threat-and-mitigations.cfm
- Category: Supporting Documents > FAQ
- SHA256: A21522119003950A314994BCEE67A6E6FEB9EA92D8E48FF5980555B0AA4C6DB2
- Size: 316KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Best Practices for Keeping Your Home Network Secure

- Abstract: Electronic computing devices including computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars and other "Internet of Things" devices must all be secured in order to prevent attack. Most home entertainment and utility devices, such as home monitoring systems, baby monitors, Internet of Things (IoT), Smart Devices, Blu-ray players, streaming video players, and video game consoles are capable of accessing the Internet, recording audio, and/or capturing video. Implemented security measures can ensure these devices don't become the weak link in your home protection.
- Date: 09/26/2018
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/faq/best-practices-for-keeping-your-home-network-secure.cfm
- Category: Supporting Documents > FAQ
- SHA256: D96931DCEF3EF5963CE5940710E0BF86D1BC20708C04CA351D38EE914E47A29D
- Size: 291KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

A Guide to Border Gateway Protocol (BGP) Best Practices

- Abstract: The dominant routing protocol on the Internet is the Border Gateway Protocol (BGP). BGP has been deployed since the commercialization of the Internet and version 4 of BGP is over a decade old. BGP works well in practice, and its simplicity and resilience enabled it to play a fundamental role within the global Internet. However, BGP inherently provides few performance or security protections. With BGP being the primary protocol driving the Internet, the security of devices dedicated to running the protocol is vital. Unfortunately, there are many vulnerabilities that can be exploited if proper mitigations are not configured. This error seems to be far more common than it should. For that reason this guidance paper is provided.
- Date: 09/17/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/a-guide-to-border-gateway-protocol-bgp-best-practices.cfm
- Category: Reports
- SHA256: FCC3E54DB7CC8F51C00B0FA3991579CF846B90955A5CA1BB444C8B5D30940679
- Size: 222KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Best Practices for Keeping Your Home Network Secure

- Abstract:
- Date: 09/01/2018

- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf
- Category: Info Sheet
- SHA256: 125C8C30AAAE99FEA3307977B94133D97489657023233C6AF3BB7411C1FA7718
- Size: 577KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

A Guide to Border Gateway Protocol (BGP) Best Practices

- Abstract:
- Date: 09/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-guide-to-border-gateway-protocol-best-practices.pdf
- Category: Tech Report
- SHA256: 27F10858D428C667C15A9E08D53C1ACD8296D4650475CF93646C556E6125ADB8
- Size: 1,117KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Identity Theft Threat and Mitigations

- Abstract:

- Date: 09/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-indentity-theft-threat-and-mitigations.pdf
- Category: Info Sheet
- SHA256: A4C4FAC93E75CF1B723F7313D114BF2E785A04AF0882494A5DA07BA326F5DECA
- Size: 789KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Cloud Security Basics

- Abstract: Cloud services provide enterprise organizations flexibility and new capabilities, however they introduce new risks that must be understood and addressed before procuring a cloud service provider (CSP). Department of Defense (DoD) organizations are charged with handling sensitive data ranging from Personally Identifiable Information (PII) to national security information. As more sensitive data is considered for storage and manipulation in cloud environments, organizations must address new security threats before deploying in an operational environment.
- Date: 08/29/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/cloud-security-basics.cfm
- Category: IA Guidance > Security Tips
- SHA256: 893077B6054F891039D23E04841792DC7C08814A361884705F649BC33F75DF85
- Size: 215KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cloud Security Basics

- Abstract:
- Date: 08/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-cloud-security-basics.pdf
- Category: Info Sheet
- SHA256: 776792EF1B0DDC8FC4473EFB46A7253BE8054CE6AAD05750E0180F9DDB827E40
- Size: 628KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Blocking Unnecessary Advertising Web Content

- Abstract: Cyber adversaries can leverage malicious advertising (“malvertising”) to install malware. Exploit kits in malicious ads can take advantage of unpatched vulnerabilities to silently install malware. Administrators should ensure that software updates are implemented promptly to prevent malware installation. Blocking potentially malicious web advertisements further mitigates malvertising. Additionally, blocking such content can decrease traffic across the network boundary, streamlining incident forensics and enhancing network performance.
- Date: 07/10/2018
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/blocking-unnecessary-advertising-web-content.cfm
- Category: Supporting Documents
- SHA256: E42B47B5A620224DC151FF8B3B42917A5A27C050C44D5104912CDFD7D170C01D
- Size: 203KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Blocking Unnecessary Advertising Web Content

- Abstract:
- Date: 07/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-blocking-unnecessary-advertising-web-content.pdf
- Category: Info Sheet
- SHA256: 1B34EBEC3E27CCB7155C61F8A36EE70AAA06D4006DAAD50B4807500B83F81E10
- Size: 505KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

WPA3 will Enhance Wi-Fi Security

- Abstract: On January 8th 2018, the Wi-Fi alliance announced new enhancements to Wi-Fi Protected Access II (WPA2) security specification and a new WPA3 security specification. Enhancements to WPA2 will include improvements in authentication, encryption, and configuration requirements. WPA3 will build on the WPA2 enhancements and will offer enhanced protection for Wi-Fi networks that use password-based authentication, improved privacy on open networks, mitigations against denial-of-service attacks, and will deliver stronger cryptographic strengths that comply with Commercial National Security Algorithm (CNSA) requirements. A mechanism to provision IoT devices with limited or no displays into the network will also be introduced along with WPA3.
- Date: 06/28/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/wpa3-will-enhance-wi-fi-security.cfm

- Category: Reports
- SHA256: EEEA5D1699E35A5930A187928D88DF4836C900D68DA74286AB75F3479AF3CDAD
- Size: 441KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mobile Device Best Practices When Traveling OCONUS

- Abstract: In their brief history, mobile devices have evolved to become the critical link between a remote user and the home office, providing travelers with access to business applications and data they would otherwise lack. Ensuring that this line of communication is private and secure is imperative. The security guidance outlined below applies to U.S. Government personnel using Government-issued commercial mobile devices in a public network as they travel in foreign countries. The purpose is to minimize an adversary's ability to obtain sensitive data through mobile devices and limit damage should one be compromised. The mitigations address a range of threats that might be encountered in foreign countries.
- Date: 06/07/2018
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/mobile-device-best-practices-when-traveling-oconus.cfm
- Category: Supporting Documents
- SHA256: 25E996411BD23C0B3F8E406078F159C0BCB358D1EDE0058B23F646A2C7A74BAE
- Size: 234KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

How to fulfill the Requirement to Upgrade Symantec Proxy CAS

- Abstract:
- Date: 06/01/2018
- Link: https://apps.nsa.gov/PartnerLibrary/CSA_How_to_Fulfill_the_Requirement_to_Upgrade_Symantec_Proxy_CAS.pdf
- Category: Advisory
- SHA256:
- Size:
- Location: Current
- Access Controlled: True

Return to the Table of Contents.

WordPress Plugin WP Symposium Remote Code Execution CVE-2014-10021

- Abstract:
- Date: 06/01/2018
- Link: https://apps.nsa.gov/PartnerLibrary/CSA_Cybersecurity_Advisory_Wordpress_Symposium.pdf
- Category: Advisory
- SHA256:
- Size:
- Location: Current
- Access Controlled: True

Return to the Table of Contents.

WPA3 Will Enhance Wi-Fi Security

- Abstract:

- Date: 06/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-cybersecurity-technical-report-wpa3.pdf
- Category: Tech Report
- SHA256: 4FB0E3FA574F33AA33E2FD7F146664224961B10CE3551B07AC8410CDCA78B89E
- Size: 709KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Steps to Secure Web Browsing

- Abstract: Web browsers pose a unique risk to enterprise infrastructure because of their frequent exposure to untrusted dynamic content. Configuring browser security settings is challenging due to uncertainty of both attack mitigation effectiveness and impact on end users. A key goal of this paper is to avoid impact to users while mitigating as many attacks as possible. The following guidance uses a statistics-based approach to identify three mitigations in commonly-used web browsers that, in combination, will ward off nearly all publicly known attacks. Further mitigations are provided at the end of the document for administrators seeking to defend against adversaries with significant resources.
- Date: 05/18/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/steps-to-secure-web-browsing.cfm
- Category: Reports
- SHA256: FB41B117D2AA411F4684575203412A0BE5DA3CFE99128F00EB5636CB09E2D4CB
- Size: 135KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mobile Device Best Practices When Traveling OCONUS

- Abstract:
- Date: 05/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-mobile-device-best-practices-when-traveling-oconus.pdf
- Category: Info Sheet
- SHA256: 7D1E51C6E12E441D7CA3440330F5816506F732F3D89CFAAAF51F01D5ED18E497
- Size: 319KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Steps to Secure Web Browsing

- Abstract:
- Date: 05/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-steps-to-secure-web-browsing.pdf
- Category: Info Sheet
- SHA256: 59B21F04A3EEF8897432283EC5404A331F5F5AF4587740CC4A309F1A359EB9AB
- Size: 461KB
- Location: Current

- Access Controlled: False

Return to the Table of Contents.

Drupal Unauthenticated Remote Code Execution Vulnerability CVE-2018-7600

- Abstract: On March 28, 2018, the Drupal project announced that a vulnerability had been discovered in Drupal 7.x and 8.5.x (as well as prior, unsupported versions) that allows an unauthenticated attacker to execute arbitrary commands on Drupal installations. In some situations, Drupal installations not directly connected to the Internet could be vulnerable to exploitation through a Cross-Site Request Forgery (CSRF) attack.
- Date: 04/23/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/drupal-unauthenticated-remote-code-execution-vulnerability.cfm
- Category: IA Advisories
- SHA256: 61D612D03766FC45C3DB020B5631295A5B19447FD71710980040D8217118FC50
- Size: 119KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Multiple Critical Vulnerabilities Identified in Cisco Smart Install

- Abstract: Cisco recently released multiple critical vulnerabilities associated with the Smart Install Protocol (CVE-2018-0171 and CVE-2018-0156). The two CVEs cover remote code execution and Denial of Service vulnerabilities due to malformed Smart Install packets. This is a followup to a previously released IAA advising users to not use the insecure Smart Install protocol (IAA U/OO/801020-17).
- Date: 04/09/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/multiple-critical-vulnerabilities-identified-in-cisco-smart-install.cfm

- Category: IA Advisories
- SHA256: 34AEBC2B71A10A228424C8498C7AF077C2900C75B735D413EBFC555EFC195328
- Size: 493KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Windows 10 for Enterprises Security Benefits of Timely Adoption

- Abstract: This document describes features present in Windows 10 Enterprise 64-bit that can disrupt exploitation techniques and tools used against National Security Systems today and how the timely adoption of new releases can help to protect systems in the future. The functionality of many of these features has been evaluated through the National Information Assurance Partnership (NIAP).
- Date: 04/06/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/windows-10-for-enterprises-security-benefits-of-timely-adoption.cfm
- Category: IA Guidance > Security Tips
- SHA256: D2B4DF4B06D61D40D37095083D5E00DFBFD100D4B933D14217FC153C4A21D1CD
- Size: 280KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Seven Steps to Effectively Defend Industrial Control Systems

- Abstract: Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICS), it's not a matter of if an intrusion will take place, but when. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.
- Date: 04/06/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/seven-steps-to-effectively-defend-industrial-control-systems.cfm
- Category: Reports
- SHA256: 8C9FB5FC0B66B0CA4EF553BDCAAB698241DB48FD0FFAC775AA321E56061FFFD8
- Size: 797KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Windows 10 for Enterprises Security Benefits of Timely Adoption

- Abstract:
- Date: 04/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-windows-10-for-enterprise-security-benefits-of-timely-adoption.pdf
- Category: Info Sheet
- SHA256: C0C95BFC57205F94170DCF6C0D2F499CCD5B58C51341EF732580A180DA3FE08F
- Size: 379KB
- Location: Current

- Access Controlled: False

Return to the Table of Contents.

Multiple Critical Vulnerabilities Identified in CISCO Smart Install

- Abstract:
- Date: 04/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/orn-cisco-smart-install.pdf
- Category: ORN
- SHA256: BDCC84CA316E6397E045FF72A998455593530AA3EF3E987AC1450C0C158DE13A
- Size: 451KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Drupal Unauthenticated Remote Code Execution Vulnerability

- Abstract:
- Date: 04/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-drupal-remote-code-execution-vulnerability-cve.pdf
- Category: Advisory
- SHA256: 44DD85285D2F319F653168DA185D10CD26515DED335DDC11DA8D1E4F9D1D740C
- Size: 289KB
- Location: Current

- Access Controlled: False

Return to the Table of Contents.

UNFETTER

- Abstract: Unfetter is bringing Net Defenders and Threat Analysts together for the first time. Net Defenders need the ability to make operational decisions based on complex threat data published by Threat Analysts. A unique platform that unifies the Net Defender and Threat Analyst communities, Unfetter breaks down barriers through seamless data sharing across the enterprise. By enabling the real-time exchange of threat data and analytics based on the MITRE ATT&CKTM Framework, Unfetter allows organizations to evaluate and implement defensive measures based on effectiveness and value.
- Date: 03/29/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/unfetter.cfm
- Category: IA Guidance > Security Tips
- SHA256: 73E7B23FE2D1C78AA751F0E0FB4E8188FB537BCD4B160F449A36548899A508DF
- Size: 730KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

NSA/CSS Technical Cyber Threat Framework v1

- Abstract: This framework was designed to help NSA characterize and categorize adversary activity by using a common technical lexicon that is operating system agnostic and closely aligned with industry definitions. This common technical cyber lexicon supports sharing, product development, operational planning, and knowledge driven operations across the IC. Public dissemination of the technical cyber lexicon allows for collaboration within the whole community. Use of the NTCTF facilitates organizing and examining adversary activity to support knowledge management and enable analytic efforts.

- Date: 03/08/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/nsa-css-technical-cyber-threat-framework-v1.cfm
- Category: Reports
- SHA256: 49E1DAC671D980DA612BDBFFBE224E7AEF3EB5D70017FF1CC385AF039C7D01F1
- Size: 1,275KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

NSAs Top Ten Cybersecurity Mitigation Strategies

- Abstract: NSA's Top Ten Mitigation Strategies counter a broad range of exploitation techniques used by Advanced Persistent Threat (APT) actors. NSA's mitigations set priorities for enterprise organizations and required measures to prevent mission impact. The mitigations also build upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and promote a defense-in-depth security posture. The mitigation strategies are ranked by effectiveness against known APT tactics. Additional strategies and best practices will be required to mitigate the occurrence of new tactics.
- Date: 03/06/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm
- Category: IA Guidance > Security Tips
- SHA256: FF066507B744A2899043D55B0E90027DCE0422F07F040F9308D68DAF717C17A8
- Size: 194KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

NCTOC Top 5 Security Operations Center (SOC) Principles

- Abstract:
- Date: 03/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/nctoc-top-5-soc-principles.pdf
- Category: Info Sheet
- SHA256: 0186E633981F22489DB0AA37FA207BB2082C4F096E549B83336F0EF30CE4C5CE
- Size: 126KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

UNFETTER

- Abstract:
- Date: 03/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-unfetter.pdf?v=2
- Category: Info Sheet
- SHA256: 9E02DDD94B7EB225820981A4808C3C78808746A4B7E5048DAA7A6044F3017719
- Size: 494KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Top 10 Mitigation Strategies

- Abstract:
- Date: 03/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf
- Category: Info Sheet
- SHA256: 7A22DDD95E75CC9E44B229480F9C346F0044BDB829A36651AED11251AD69B12D
- Size: 348KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

UEFI Lockdown Quick Guidance

- Abstract:
- Date: 03/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-uefi-lockdown.pdf
- Category: Info Sheet
- SHA256: D428CF61940FC2BC9D63BA8E58525E2B56D34752B8B6816788602ED9EF08E7E5
- Size: 416KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

UEFI Advantages Over Legacy Mode

- Abstract:
- Date: 03/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-uefi-advantages-over-legacy-mode.pdf
- Category: Info Sheet
- SHA256: 6A3C09457B3726B033BA306BDC7EE95C88DDD71E6F94A3FFF1129D7C4878DF33
- Size: 336KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Unified Extensible Firmware Interface (UEFI) Advantages

- Abstract: Device vendors have redefined the interface between the OS and platform firmware. The interface, defined in various UEFI specifications, replaces the older Basic Input/Output System (BIOS). Old BIOS computers need to be replaced, and newer UEFI computers should switch to UEFI native mode for several technical advantages: Secure Boot; GUID Partition Table (GPT) Support; Platform and Architecture Independence; Consistent Variables and Services; Improved Boot Performance.
- Date: 02/07/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/cfs-u-oo-111747-18.cfm
- Category: IA Guidance > Security Tips
- SHA256: 1E4DE2E77D7DD36C218A923519CD21DCB311F5ABA8A086BB167CF3DC4C4172F4
- Size: 352KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cisco Updates Critical Remote Code Execution Vulnerability Advisory for ASA

- Abstract: Cisco recently updated a vulnerability advisory affecting Cisco Adaptive Security Appliance (ASA) and Firepower Appliance, CVE-2018-0101. The updated release informed users that devices continue to be vulnerable after the 29 January 2018 advisory and software release. Furthermore, Cisco disclosed the existence of additional vulnerable features. The updated advisory, released 5 February 2018, recommends users again install updated software since the versions released on 29 January 2018 do not include fixes for the newly disclosed vulnerabilities. This IAA addresses Cisco ASA vulnerabilities in CVE-2018-0101.
- Date: 02/07/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/iaa-u-oo-11303-18.cfm
- Category: IA Advisories
- SHA256: 7331277943368231CA4487E525D0A5712AEBD1890F29E2EAC7B45A4283E7EF0E
- Size: 197KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

CISCO Updates Critical Remote Code Execution Vulnerability for ASA

- Abstract:
- Date: 02/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-cisco-asa-cve.pdf
- Category: Advisory
- SHA256: 929E50857498FE8E5AA6200127238BCEDE0351D0BFE3DFC4E844543D7285782E
- Size: 283KB

- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Exchangeable Image Format (EXIF)

- Abstract: Exif is structured, tagged metadata contained within some media file formats. This data is used by digital camera manufacturers and applications that process digital images to provide additional information about media files. The metadata includes manufacturer specific information such as the make, model and lens information of the device that generated the file; image information (e.g. date/time of capture) and geolocation information (e.g. latitude/longitude) can also be recorded. Exif data is found in two image standards: Joint Photographic Experts Group (JPEG) File Interchange Format (JFIF) (as defined in International Standards Organization/International Electrotechnical Commission (ISO/IEC) 10918-1) and TIFF Revision 6.01. The Exif format is also defined for audio files in the format of Resource Interchange File Format (RIFF) Waveform Audio File Format (WAVE). This guidance document examines the Exif specifications for data attack, data hiding, and data disclosure risks that exist within the metadata structure. It provides a breakdown of each component of Exif metadata and provides recommendations that can help assure that Exif data is not only compliant with the specifications, but also free of risk.
- Date: 02/01/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/inspection_and_sanitization_guidance_for_exchangeable_image_format.cfm
- Category: Reports
- SHA256: 8A7D792870CEB303BB17DCAC650C20D66F9633DAE657326A3C42B932104E3E4C
- Size: 933KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for the DOD Electronic Biometric Transmission Specifications (EBTS) File Format

- Abstract: The purpose of this document is to provide guidance for the development of sanitization and analysis software for Department of Defense (DOD) Electronic Biometric Transmission Specification (EBTS) biometric files. This document analyzes elements and objects contained within the EBTS file structure and then discusses the data hiding, data attack, and data disclosure risks. It describes how identified elements can be a cause for concern for hiding sensitive data to ensure EBTS files are safer for users to open and conform to the specification.
- Date: 02/01/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/inspection_and_sanitization_for_dod_ebts_file_format.cfm
- Category: Reports
- SHA256: 11FE11F0EEBFA30994DD1440FC70F26746E8E6C11FC715B1F477335CE602BECD
- Size: 1,672KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Analysis of Optical Character Recognition (OCR) Techniques for Security Marking Detection

- Abstract: This document deconstructs the problem of automated character recognition and defines a methodology for conducting optical character recognition (OCR) on images for boundary protection devices to determine their classification. This research can be leveraged in order to make determinations on the transfer of images between security domains.
- Date: 02/01/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/analysis_of_optical_character_recognition_techniques.cfm
- Category: Reports
- SHA256: A8C38EF0B296A1F3FC8C1C5CBA47F79917C712FE3FA813BEA1F171C2EBD3C63D

- Size: 979KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Guidance for JSON and JSON Schema

- Abstract: This paper provides guidance for creating JSON schemas. Validating JSON instance documents against properly designed JSON schemas can reduce the risk of transferring unauthorized or malicious data. Note that schema validation alone is not enough to prevent transfer of unauthorized data; users must perform other content filtering such as dirty word and anti-virus checks, in conjunction with schema validation.
- Date: 02/01/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/security_guidance_for_json.cfm
- Category: Reports
- SHA256: 347F2BFD7A276C1075A6159FDBC65283599ED9F63CC5A43A911A20CD2A289BA9
- Size: 880KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for PNG

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization or analysis software tool for Portable Network Graphics (PNG) files. This document analyzes the various elements contained within the PNG images and then discusses data attack, data disclosure, and data hiding risks. It describes how these elements can then be a cause for concern from

hidden sensitive data or from attempts to exploit a system. This report provides numerous recommendations and mitigations that could be used to ensure the use of PNG is safe and that files conform to the specification.

- Date: 02/01/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/inspection_and_sanitization_guidance_for_png.cfm
- Category: Reports
- SHA256: 86EF456BC3323D3FFF0660A9CE37FB318D21E4967CEF82BF3937690304906CB0
- Size: 931KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for MPEG-2

- Abstract: MPEG-2 is a standard for the generic coding of moving pictures and associated audio information. It describes a combination of lossy compression methods for storage and transmission of audio and video using available storage media and transmission bandwidth. It includes an analysis of the issues with the H.264 advanced video coding, part 10 of MPEG-4. It also provides for inclusion of metadata such as Key-Length-Value, which can be obtained from unmanned aerial vehicle platforms capturing motion imagery. The MPEG-2 standard contains detail down to the bit level, fields that include metadata, conditional information, and variable length content require inspection to ensure data is not hidden or unintentionally disclosed. Given the typically large amount of data contained in MPEG-2 files, inspection and sanitization are critical to ensure that all content within the files can be displayed to end users and that files have no malicious content.
- Date: 02/01/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/inspection_and_sanitization_guidance_for-mpeg-2.cfm
- Category: Reports
- SHA256: 7CCC0827D1C9038E03945D05178CCFB3A73C56431A54602370A4CAE4A5BCCEF5

- Size: 2,887KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

UEFI Lockdown Quick Guidance

- Abstract: Unified Extensible Firmware Interface (UEFI) provides multiple levels of password-based boot control. Three password levels are used to interact with machine firmware prior to the operating system boot. Failure to secure these accounts can open machines up to unauthorized, undesired, and repudiated boot device changes, device/component firmware configuration changes, and unauthorized connectivity to peripheral devices.
- Date: 01/25/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/uefi_lockdown_quick_guidance.cfm
- Category: IA Guidance > Security Tips
- SHA256: F4EC2715ECE77CE2E82706BEA7B701B8423B2F5916070AB11EAA6E59F32CEC3C
- Size: 464KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Verification, Inspection, and Sanitization Report Specification

- Abstract: The Verification, Inspection and Sanitization (VIS) Report Specification provides a standardized XML-based mechanism to describe the results of all the verification, inspection, sanitization, transformation, and transliteration filter actions performed by a Filter Orchestration Engine (FOE) and its associated filters on a given set of data. The initial use case for the VIS report Specification was to support the filter reporting requirements of the Filter Sidecar Protocol (FSP). However, a VIS Report has general applicability to any

system (or component) performing filtering including local and distributed filters, filter orchestration engines, Filter Sidecars, Cross Domain Solutions (CDS), and other boundary protection devices (e.g. firewalls, web proxies, mail gateways).

- Date: 01/19/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/verification-inspection-and-sanitization-report-specification.cfm
- Category: Reports
- SHA256: 9A138EA75CB23601F586F021A1DC571C8D4490B804F0151B5A30147888F35585
- Size: 682KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Unicode Security Risks

- Abstract: Fundamentally, computers process numbers, not letters, so when a computer processes text, the characters must be converted into numbers prior to processing. There are many schemes for encoding characters as numbers. US-ASCII is one well-known scheme, but it encodes only the English (Latin) alphabet. By contrast, Unicode is an international standard that assigns a unique number to each of the characters in the world's languages. This document provides a brief overview of Unicode and discusses the potential security risks posed by using Unicode. It includes background on the growth of Unicode, definitions of commonly used Unicode terms, tips for creating filters to avoid visual spoofing attacks, and links to tools and further information.
- Date: 01/19/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/unicode-security-risks.cfm
- Category: Reports
- SHA256: 3F0F69504B8A80FED5554DB147A11078D745A6E94802319B5D426C82F5982460
- Size: 715KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for National Imagery Transmission Format (NITF)

- Abstract: This Inspection and Sanitization Guidance (ISG) for National Imagery Transmission Format (NITF) document provides guidelines and specifications for developing file inspection and sanitization software for NITF files, which are formally defined by the National Imagery Transmission Format Standard (NITFS). The latest NITF 2.1 standard is defined in MIL-STD-2500C. NITF files contain numerous segments of data that include images, graphics, text, as well as custom data in a strict format. As with prior ISG documents, this document is concerned with data hiding, data disclosure, and data attack risks. For example, although the NITF standard is well-defined and contains detail down to the byte level, there remain fields that include metadata, conditional information, and variable length content that require inspection to ensure nothing is hidden within the file. The nature of NITF files is to include a variety of imagery and associated data that could potentially be displayed to an end user. Information can be selectively displayed to the user based on capability and the information that was requested. With potentially a large amount of data located in these files, inspection and sanitization is key to ensuring that information contained in the file is authorized for display to the user and that the data cannot be used to attack the system.
- Date: 01/19/2018
- Link: https://apps.nsa.gov/iaarchive/library/reports/inspection-and-sanitization-guidance-for-national-imagery-transmission-format.cfm
- Category: Reports
- SHA256: 85B89926B210A40A36309AC98C1087D197A5F62D68CCF69058BF21BD72F484E8
- Size: 1,116KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

DotNetNuke Remote Code Execution Vulnerability CVE-2017-9822

- Abstract: DotNetNuke (DNN), also known as DNN Evoq and DNN Evoq Engage, is a web-based Content Management System (CMS) developed on the Microsoft .NET framework. DNN is a web application commonly deployed on local or cloud Microsoft IIS servers. On July 7, 2017, security researchers revealed a vulnerability within DNN versions 5.2.0 through 9.1.0 that allows an attacker to forge valid DNN credentials and execute arbitrary commands on DNN web servers.
- Date: 01/09/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/dotnetnuke-remote-code-execution-vulnerability-cve2-2017-9822.cfm
- Category: IA Advisories
- SHA256: 0641E3C9183180EDD9139D97152E31334F7B11B206DFED7156328DA0679CE73E
- Size: 339KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Vulnerabilities Affecting Modern Processors

- Abstract: Three vulnerabilities affecting modern Intel, AMD, and ARM processors have been disclosed. CVE-2017-5753 (bounds check bypass) and CVE-2017-5715 (branch target injection), also known as Spectre, have been confirmed to affect Intel, AMD, and ARM processors. CVE-2017-5754 (rogue data cache load), also known as Meltdown, has been confirmed to affect Intel processors. The vulnerabilities could be leveraged to read privileged system memory from an unprivileged context. The vulnerable processors are present in systems widely used across the Department of Defense (DoD). Software patches have been released by vendors to mitigate the hardware vulnerabilities.
- Date: 01/06/2018
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/vulnerabilities_affecting_modern_processors.cfm
- Category: IA Advisories
- SHA256: 5B3AC55B4A2721D542BC273816E9013D466EDC4B7F4680510D6305768A3F906F

- Size: 288KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Vulnerabilities Affecting Modern Processors

- Abstract:
- Date: 01/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-vulnerabilities-affecting-modern-processors.pdf
- Category: Advisory
- SHA256: 5ECF6159CEE509A7748FBA81CBD68DAE8315AEB572595CEF48FCEE2020F92C0D
- Size: 512KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

DotNetNuke Remote Code Execution Vulnerability

- Abstract:
- Date: 01/01/2018
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-dotnetnuke.pdf
- Category: Advisory
- SHA256: FE4EDDF830CBECE0D90351A7E257E0841451369FC9CC1A0A91EE5B7EC703C0D9

- Size: 353KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Securing Kernel Modules on Linux Operating Systems

- Abstract: The Linux kernel is the core component of a family of Operating Systems (OS) that underpins a large number of government and commercial servers and infrastructure devices. Kernel functionality is commonly enhanced through the use of modules, which can be loaded at boot time or during normal system operation. Modules run at the same privilege level as the kernel. Any vulnerabilities in kernel modules present a serious risk. System owners are advised to 1) ensure that only signed kernel modules are loaded, and 2) prevent loading of unnecessary kernel modules. Although it reduces attack surface, preventing module loading is not practical for many general-purpose systems and thus is not suitable for use in compliance baselines.
- Date: 12/16/2017
- Link: https://apps.nsa.gov/iaarchive/library/reports/securing-kernel-modules-on-linux-operating-systems.cfm
- Category: Reports
- SHA256: 07461C562D137F680029ABE58B388D473910474E62FB582B1A3096317552EE7F
- Size: 238KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Bro NSM Hunting Tips

- Abstract: The Bro Network Security Monitor (NSM) is used on networks worldwide for in-depth network monitoring and hunting for potential malicious activities. This document provides tips for analysts on how to raise a notice when irregular activity is observed on a

network.

- Date: 12/13/2017
- Link: https://apps.nsa.gov/iaarchive/library/reports/bro-nsm-hunting-tips.cfm
- Category: Reports
- SHA256: 5BB9DD43E796E4FD5C537075480C60818203526448F4CDB127757A99034832E3
- Size: 1,141KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

RSA SecurID Token Authentication Agent Vulnerabilities

- Abstract: A recent error handling vulnerability has been discovered in two RSA (Rivest Shamir Adleman) Authentication Agent toolkits and in one Authentication Agent product. This vulnerability can result in authentication bypass and affects a limited number of applications. These toolkits and product are used to deploy RSA SecurID Token Authentication to authenticate users to workstations, web servers, and network devices.
- Date: 12/13/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/rsa-securid-token-authentication-agent-vulnerabilities.cfm
- Category: IA Advisories
- SHA256: 4C3B9E7DB35C20D71DFC3D9A94EA490E7909F699C63547F6F4FC9DF11584DC2E
- Size: 226KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

RSA SecureID Token Authentication Agent Vulnerabilities

- Abstract:
- Date: 12/01/2017
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-rsa-securid.pdf
- Category: Advisory
- SHA256: 030A20DB44063D2D70DB49E417F5658375CF59E1D8CFA78CAED7479A0CC1BFC1
- Size: 392KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for TIFF File Formats

- Abstract: The purpose of this Inspection, Sanitization, and Guidance (ISG) document is to provide guidance for the development of a sanitization and analysis software tool for different versions of Tag Image File Format (TIFF), BigTIFF, and GeoTIFF. This document analyzes various elements and objects that are contained within the TIFF file structure and then discusses data hiding, data attack, and data disclosure risks. It will describe how these elements can be a cause for concern from hidden, sensitive data or from possible attempts to exploit a system. This document provides numerous recommendations and mitigations that could be used to ensure the TIFF file is safer and more accurately conforms to the specification.
- Date: 11/17/2017
- Link: https://apps.nsa.gov/iaarchive/library/reports/tiff_inspection_and_sanitization_guidance_v1_1_1-20171206.cfm
- Category: Reports
- SHA256: 8CB9094ACB55D8D31BE63597C46FA742CDCD2C089B0787C1042E46DDFE257906
- Size: 1,334KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

RSA Key Generation Vulnerability Affecting Trusted Platform

- Abstract: A vulnerability in a cryptographic library used to generate Rivest-Shamir-Adleman (RSA) encryption keys was recently disclosed. The vulnerability allows recovery of a private key when only possessing a public key. The vulnerable library is included in the firmware of specific Infineon Trusted Platform Modules (TPM) present in systems produced by a number of Original Equipment Manufacturers (OEM) commonly used in the Department of Defense (DoD). Much of the published guidance focuses on Windows but the vulnerability is not in Windows. All systems and devices that include or use the vulnerable library are affected.
- Date: 10/25/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/rsa-key-generation-vulnerability-affecting-trusted-platform.cfm
- Category: IA Advisories
- SHA256: 066C7462C752A1AD944F8D7169FEA3C1ADF0E787EC75FB9219D66BF4CCDCE890
- Size: 271KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mitigations for Key Reinstallation Attacks Against Wi-Fi Protected Access II (WPA2)

- Abstract: On October 16, 2017, a vulnerability in the Wi-Fi Protected Access II (WPA2) mechanism used for authentication and session key agreement was released. The vulnerability affects the following WPA2 handshakes: the Four-way, Group Key, Fast BSS Transition (FT), Peerkey, TDLS, and WMN Sleep Mode Response handshakes.
- Date: 10/18/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/mitigations-key-reinstallation-attacks-against-wpa2.cfm

- Category: IA Advisories
- SHA256: 7F0ED294770F4769FFE2102E140FB021C72D858C29A3D40A705246150527E563
- Size: 101KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mitigations for Key Reinstallation Attacks Against WI-FI Protected Access II (WPA2)

- Abstract:
- Date: 10/01/2017
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-mitigations-for-key-reinstallation-attacks-against-wifi-access-ii.pdf
- Category: Advisory
- SHA256: 98502C145C5E4F10FA168F288C665DE1CB495362B71C08C07913C2DC5F5AB8A8
- Size: 338KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

RSA Key Generation Vulnerability Affecting Trusted Platform Modules

- Abstract:
- Date: 10/01/2017

- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-rsa-key-generation-vulnerability-affecting-trusted-platform-modules.pdf
- Category: Advisory
- SHA256: 8EEE3C3F4E7F87D920748A69C068DE178F252CC16D87852F7D7E09A2E75688D6
- Size: 342KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Cisco Smart Install Protocol Misuse

- Abstract: Adversaries are likely exfiltrating copies of configuration files on internet accessible switches using the Cisco Smart Install functionality. This protocol exposes infrastructure devices to increased operational risk, which could compromise device integrity. Malicious Smart Install protocol messages can allow an unauthenticated, remote attacker to change the startup-config file, force a reload of the device, load a new IOS image on the device, and execute high-privilege CLI commands on switches running Cisco IOS and IOS XE Software.
- Date: 08/11/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/cisco-smart-install-protocol-misuse.cfm
- Category: IA Advisories
- SHA256: 38084F7B32399DEA30A1C41502AF9D0FF6FD0FCA92815ECF530977AB402B98EC
- Size: 270KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

CISCO Smart Install Protocol Misuse

- Abstract:
- Date: 08/01/2017
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-cisco-smart-install-protocol-misuse.pdf
- Category: Advisory
- SHA256: F463E38F9B337A53E6C86611F449892AF958DFADB4A56F5981F8B67A6ED4B1A7
- Size: 357KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Security Guidance for the Use of JSON and JSON Schemas

- Abstract: This paper provides guidance for creating JSON schemas. Validating JSON instance documents against properly designed JSON schemas can reduce the risk of transferring unauthorized or malicious data. Note that schema validation alone is not enough to prevent transfer of unauthorized data; users must perform other content filtering such as dirty word and anti-virus checks, in conjunction with schema validation. The intended audience of this paper includes system engineers, designers, and testers who work with JSON and/or JSON schemas.
- Date: 07/26/2017
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/security-guidance-use-json-andjson-schemas.cfm
- Category: Supporting Documents
- SHA256: 3E4BB3F0E7D09EE348F59EABFAFF21AFF05E14ACA88517C086991C012F8378FC
- Size: 1,041KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Juniper Network Announces Multiple Critical Vulnerabilities

- Abstract: Juniper Networks recently published 22 security advisories for Junos OS and ScreenOS, at least four advisories are “critical” and 11 are “high” severity. Some of the reported vulnerabilities can affect Junos OS across all products and platforms. These vulnerabilities could result in denial of service, remote code execution, privilege escalation, or unauthorized access.
- Date: 07/14/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/juniper-network-announces-multiple-critical-vulnerabilities.cfm
- Category: IA Advisories
- SHA256: B1B2054992D0A7B0BDA8A3C81C4806D597AFFF4595C3566B37F84E954CF9B958
- Size: 190KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

UEFI Defensive Practices Guidance

- Abstract:
- Date: 07/01/2017
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-uefi-defensive-practices-guidance.pdf?ver=2018-11-06-074836-090
- Category: Tech Report
- SHA256: 12981735FECCB4472B633243DF4CAA651D8BD39E97B07D037EF7D4DCC5808571

- Size: 1,790KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Cisco Simple Network Management Protocol Buffer Overflow Vulnerabilities

- Abstract: Various Cisco product lines are affected by buffer overflow vulnerabilities in the underlying SNMP platform. According to Cisco, these vulnerabilities can allow attackers with knowledge of community strings or passwords to gain remote code execution on routers or conduct denial of service attacks. Vulnerabilities are exploitable if SNMP is enabled and authentication is successful. To ensure a Cisco router is not at risk, MIBs and software versions need to be immediately checked for a wide range of affected products. The MIB whitelisting mitigation actions listed in this IAA should be implemented regardless of platform and operating system version.
- Date: 06/30/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/cisco-snmp-buffer-overflow-vulnerabilities.cfm
- Category: IA Advisories
- SHA256: 251B8AEB7A375F85E99C4ECD0FFC99C3686D77F12EB1BB251C21A03AF2DA3B99
- Size: 119KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Frank B Rowlett Award for Organizational Excellence

- Abstract: Nomination Procedures for Rowlett Awards - Group instruction booklet

- Date: 06/16/2017
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/forms-templates/rowlett-awards-organizational-excellence-nomination-procedure.cfm
- Category: Supporting Documents > Forms Templates
- SHA256: 8A4A31F378DAF4EEDB924F4DB2CDEB293A287C66D44EFD203DB063C6F62300D6
- Size: 2,425KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Devices with Intel Atom C2000 Series Processors

- Abstract: Devices with Intel Atom C2000 series processors can fail suddenly, impacting the availability of critical infrastructure and/or national security system networks. Intel Atom C2000 series processors manufactured since September 2013 (with B-0 stepping/version) could experience failure at above acceptable rates. The Low Pin Count (LPC) clock signal gradually degrades with use, potentially causing the device to cease operation and fail to boot. These processors are embedded in several types of network and enterprise devices (i.e., security appliances, network routers, and data storage devices). Suppliers are working with customers to replace or repair affected products. NSA recommends working with system suppliers as soon as possible to determine if devices are affected and create an appropriate replacement or repair strategy, depending on the criticality of the network system and use condition.
- Date: 06/16/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/devices-with-intel-atom-c2000-series-processors.cfm
- Category: IA Advisories
- SHA256: 7AFDDDB739E44913DF142CC7064FE8C7A328AFC21EB02731444D837EFC0F3DF4
- Size: 159KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program Cyber Incident Response Assistance Accreditation Instruction Manual

- Abstract: NSCAP CIRA Accreditation Instruction Manual 3.3
- Date: 06/14/2017
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/nscap-cira-accreditation-instruction-manual-3-3.cfm
- Category: Supporting Documents
- SHA256: B6354D8149663CC186402961BD06AD08109AC77A9E8B060E52AB650AED5BD4C8
- Size: 1,461KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program Accredited Companies' Contact Information

- Abstract: NSCAP CIRA-Accredited Companies' Contact Information document
- Date: 06/14/2017
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/nscap-cira-accredited-companies.cfm
- Category: Supporting Documents
- SHA256: 0EE6A30F7DC073B6B5D70ADC8CEC6512561C4905367FF90418B44978FA641E01
- Size: 86KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Advanced Concepts - Information Assurance Solutions at the Speed of Technology

- Abstract: With the accelerating pace of innovation and the convergence of new technologies such as the Internet of Things (IoT), it is increasingly difficult to manage growing IA risk. With security sometimes underinvested when bringing technologies quickly to market, potential IA vulnerabilities can be exploited at alarming rates, globally impacting civilian entities, government entities, and organizations across all industries.
- Date: 06/13/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/advanced-concepts-ia-solutions-speed-of-technology.cfm
- Category: IA Guidance > Security Tips
- SHA256: 5AE059DF0CD2F0623C79203D8C89971BFF5F83304BB3FC9A0074EA78859CE2AD
- Size: 457KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Network Security Devices Utilizing Vulnerable Weak Signature Algorithms in TLS

- Abstract: ORN-Deprecated_Signature_Algorithms
- Date: 06/02/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/network-security-devices-utilizing-vulnerable-weak-signature-algorithms-in-tls.cfm

- Category: IA Advisories
- SHA256: 1B202E4E786B11907061F7C48A69F2B98CD129A09F0E67C0EB1C42DED559A655
- Size: 505KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Network Security Devices Utilizing Vulnerable Weak Signature Algorithms in TLS

- Abstract:
- Date: 06/01/2017
- Link: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/orn-deprecated-signature-algorithms.pdf
- Category: ORN
- SHA256: E4BD6A6F21EBE34B4AE526C8DEB8C93C5A153D253D01BAD0E41451CA5A8E2A30
- Size: 527KB
- Location: Current
- Access Controlled: False

Return to the Table of Contents.

Whitelisting Windows IIS and WebDAV Traffic

- Abstract: Since web servers typically serve as the public face of an organization, they are a frequent target of attacks. For this reason, web server security is essential. Microsoft’s Internet Information Services (IIS) web server includes a Request Filtering module that

can filter HTTP requests in order to reduce a web server's attack surface. This document provides guidance on how to use Request Filtering to better secure IIS web servers through a strategy of HTTP and WebDAV verb whitelisting.

- Date: 05/19/2017
- Link: https://apps.nsa.gov/iaarchive/library/reports/whitelisting_windows_iis.cfm
- Category: Reports
- SHA256: C23777AA6D4D2EA1C93EE64B6960EE235A86A6B4DF1DC8FD521393E4779436A9
- Size: 2,003KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mitigations for WannaCrypt-WannaCry Ransomware

- Abstract: Guidance in Information Assurance Advisory No. IAA U/OO/800900-17, "March 2017 Patch Tuesday" recommended the immediate application of Microsoft's March 2017 Patch Tuesday release on all supported platforms. The release patched several zero-day vulnerabilities. In response to widespread ransomware attacks against unpatched or unsupported platforms, Microsoft has also released the same security updates for specific unsupported Windows platforms. Its immediate installation is critical for Department of Defense networks and other National Security Systems. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corp.
- Date: 05/16/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/mitigations-for-wannacrypt-wannacry-ransomware.cfm
- Category: IA Advisories
- SHA256: 452E94F21D2450CDF0EA40C6789FC85622370A663D5489469A5D022DF72DCD9F
- Size: 185KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

CVE-2017-5689: Intel AMT, Intel ISM Privilege Escalation

- Abstract: Intel published a security advisory regarding this vulnerability (Intel ID is INTEL-SA-00075). The vulnerability allows an unprivileged network attacker to perform a remote privilege escalation. It also allows an unprivileged local user to perform the privilege escalation. The vulnerability affects Intel manageability SKU platforms dating back to the 1st Generation Core architecture CPU. Intel has released detection and mitigation guidance recommending that system owners seek firmware updates from the Original Equipment Manufacturers (OEMs). The Common Vulnerabilities and Exposures (CVE) number associated with this vulnerability is CVE-2017-5689.
- Date: 05/04/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/intel-ism-privilege-escalation.cfm
- Category: IA Advisories
- SHA256: 85BDC6F673E43F98D5E547CB16C4F0CC0336E49596CD605A75FD4E6F062ABB12
- Size: 191KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Faulty Intel Atom C2000 Processor

- Abstract: The Intel Atom C2000 processor series has a critical flaw, the clock signal component degrades after 18-36 months of operational usage. As a consequence, the degradation of the processor will likely result in abrupt device failure. This processor supplies critical clock signal timing to other hardware components, including the boot ROM. These processors have been embedded in several network and enterprise devices, which provide communication security and data storage services. Vendors are cooperating

with customers to replace affected products. NSA recommends to immediately remove and replace affected devices from operational networks.

- Date: 05/03/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/faulty-intel-atom-c2000-processor.cfm
- Category: IA Advisories
- SHA256: 703CAA77C214F5468E0AFD34021703B0B46C960C9522DAF7716BF2F5869946B2
- Size: 493KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Privileged Access Management

- Abstract: Privileged Access Management (PAM) solutions protect and track the use of sensitive or critical capabilities such as administrative or service accounts. PAM solutions provide a centralized management interface for authentication and access control throughout the network. This unification provides simplified device management as well as an improved, granular least privilege implementation. In some cases, access controls and management functions can be automated.
- Date: 04/26/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/privileged-access-management.cfm
- Category: IA Guidance > Security Tips
- SHA256: 4DBAF8CA8701CB1A75D61DFAC1A7693DCF503086CCC843867902751966F1383B
- Size: 257KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Apply Kernel Protection on Windows 7 and Windows 7 SP1 - Updated

- Abstract: User mode and Kernel mode software may inadvertently or purposely access the NULL (0x00000000) memory page. This memory location has been leveraged in attacks to successfully exploit a system. Microsoft developed and released the KB28131702 patch (MS13-031) for 64-bit and 32-bit versions of Windows 7 and Windows 7 SP1 to mitigate this exploitation vector. The NULL page protection is part of Windows beginning with Windows 8 and onwards. IAVA 2013-A-0080 (KB2813170) was superseded by IAVA 2015-A-0009 and IAVA 2015-A-0033. However, those IAVAs do not address the requisite post-configuration registry value stated in the IAA document. NOTE: This document supersedes IAA-U-OO-800824-17.
- Date: 04/26/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/apply-kernel-protection-windows7-windows7sp1-updated.cfm
- Category: IA Advisories
- SHA256: 391A2170C4A7CD9DC767F5EEAE69BE3EF850433284A4C3091818C28F2110D123
- Size: 115KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Establishing NSA’s position on the use of Trusted Platform Modules in National Security Systems

- Abstract: Cryptographic components manufactured to conform to the Trusted Computing Group’s (TCG) Trusted Platform Module (TPM) specification have been widely deployed in commercial computing devices including personal computers, servers, and tablets. In 2007 the DoD Chief Information Officer issued a policy memorandum, which requires that “all new computer assets (e.g. server, desktop, laptop, and PDA) procured to support the DoD enterprise include a Trusted Platform Module (TPM) version 1.2 or higher where such technology is available.”

- Date: 04/14/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/nsa-position-trusted-platform-modules-national-security-systems.cfm
- Category: IA Advisories
- SHA256: F26AB3BDCC9587173F8257B8797BBABFE7015C9A543D858F602CA71FFEA19591
- Size: 185KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Least Privilege

- Abstract: The least privilege principle is the practice of restricting capabilities to only those who require them. On information systems, these capabilities may include: The ability to access or log into machines or services; The ability to access resources such as files or data; The ability to install, update, or execute programs, processes, or applications; The ability to add or remove users, devices, or processes to a network
- Date: 04/10/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/least-privilege.cfm
- Category: IA Guidance > Security Tips
- SHA256: 6989A36EB6032DCB6860AC42FA6F870113C1B161FB403238D8411E4C220537D6
- Size: 960KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

March 2017 Patch Tuesday

- Abstract: Microsoft's March 2017 Patch Tuesday release contains a significant number of critical patches including the delayed February Patch Tuesday patches. March's Patch Tuesday includes fixes for three publicly known zero-day vulnerabilities that have had proof of concept exploitation code available for a number of weeks. Immediate installation of all March 2017 Patch Tuesday patches is critical for Department of Defense networks and other National Security Systems.
- Date: 03/16/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/march-2017-patch-tuesday.cfm
- Category: IA Advisories
- SHA256: 3BABFBFB9EBF5CC4295988AB537284FE712D11B9584A24521AFF041C4395C3CB
- Size: 179KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Removal of Server Message Block 1.0

- Abstract: Server Message Block (SMB) 1.0 is a vulnerable, legacy file and print sharing protocol that has been deprecated by Microsoft. The SMB 1.0 protocol is susceptible to downgrade and man-in-the-middle attacks, and uses MD5 for hashing which is susceptible to collision and pre-image attacks. All supported versions of the Windows operating system support at least SMB 2.0 and do not require SMB 1.0 for regular file and print sharing functionality. At a minimum, Microsoft recommends disabling SMB 1.0, but complete removal is recommended when an operating system supports removal. If SMB 1.0 is still needed, then administrators should identify systems, devices, and software that only support SMB 1.0 and prioritize their removal, upgrade, or replacement.
- Date: 03/16/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/iaa-removal-of-server-message-block-1-0.cfm
- Category: IA Advisories
- SHA256: C302FED63C645F1EB6D1069B2D52DAFBD5133FAB50D7388ACE9D6EB82556AAB1

- Size: 230KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Overview of Software Defined Networking Risks

- Abstract: Software Defined Networking (SDN) is an emerging technology, defined by the Open Network Foundation (ONF) as “the physical separation of the network control plane from the forwarding plane, and where the control plane controls several devices.” While SDN offers new capabilities, it also introduces new risks. This document provides technical background, an overview of risks, and guidance for decision makers regarding SDN. For some networks, it may be impossible to mitigate critical risks due to architectural or implementation challenges.
- Date: 02/24/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/overview-of-software-defined-networking-risks.cfm
- Category: IA Guidance > Security Tips
- SHA256: FE5C5100925883A375ABEB779C8B23830FA985F2B96E3276A91056CB419AF327
- Size: 2,587KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Commercial Solutions for Classified Tri-fold

- Abstract: Given constantly evolving mission requirements and the rapid pace of technology advancement, protecting national security systems and deploying information assurance solutions requires an agile, scalable process. CSfC enables U.S. government customers to access the latest technologies in order to achieve their mission objectives. The CSfC process enables commercial

products to be used in layered solutions to protect classified National Security Systems (NSS) information. This provides the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

- Date: 01/31/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/commercial-solutions-for-classified-trifold.cfm
- Category: IA Guidance > Security Tips
- SHA256: 863E53325E64AA40BE7DCDEB310BB6556937B8E752F95F12D81C702722CAD5FC
- Size: 111KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Commercial Solutions for Classified Brochure

- Abstract: Given constantly evolving mission requirements and the rapid pace of technology advancement, protecting national security systems and deploying information assurance solutions requires an agile, scalable process. CSfC enables U.S. government customers to access the latest technologies in order to achieve their mission objectives. The CSfC process enables commercial products to be used in layered solutions to protect classified National Security Systems (NSS) information. This provides the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.
- Date: 01/31/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/commercial-solutions-for-classified.cfm
- Category: IA Guidance > Security Tips
- SHA256: B5F50CF7495A51C7C00903CA9A3791C9C526686CEA11F8BD78D884F39DC19762
- Size: 24,218KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Reducing the Risk of Simple Network Management Protocol Abuse

- Abstract: SNMP provides a standardized framework for a common language that is used for monitoring and managing devices in a network. This protocol relies on the usage of a secure string, referred to as a community string, which grants access to a portion of a device's management plane. There are several differences between SNMPv1, v2, and v3: SNMPv2 is nearly identical to SNMPv1, except 64-bit counters were added in order to support faster interfaces. SNMPv3 replaces the simple/clear text password sharing that was used in SNMPv2 with more securely encoded parameters. All versions run over user datagram protocol (UDP). SNMPv3 should be the only utilized version of SNMP because it has the ability to authenticate and encrypt payloads. When either SNMPv1 or SNMPv2 are utilized, the community string could be determined by an adversary by sniffing network traffic, which could then potentially lead to a man-in-the-middle and/or replay attack. Using SNMPv3 by itself is not enough to prevent abuse of the protocol. Combining SNMPv3 with a Management Information Base (MIB) whitelisting approach using SNMP views can ensure that even with exposed credentials, information cannot be read from or written to the device unless the information is needed for monitoring or normal device re-configuration. The majority of devices that support SNMP contain a generic set of MIBs that are vendor agnostic, which allows for the Object Identifier (OID) to be applied to devices regardless of manufacturer.
- Date: 01/31/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/reducing-the-risk-of-snmp-abuse.cfm
- Category: IA Advisories
- SHA256: B98D06F413398FCE49CBAF16CBBC8D939BF55FA2F7C631FFE3E2C09800FD6F92
- Size: 540KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Information Assurance Partnership 2016 Report

- Abstract: 2016 was a year of growth for National Information Assurance Partnership (NIAP) – increasing evaluated products available for National Security System procurement, collaborating with industry and government in the development of Protection Profiles which define security requirements and assurance activities for a wide range of commercial technologies, and representing the US in the Common Criteria Recognition Arrangement (CCRA), including serving as the CCRA Development Board chair.
- Date: 01/28/2017
- Link: https://apps.nsa.gov/iaarchive/library/reports/niap-2016-report.cfm
- Category: Reports
- SHA256: 27FD1EF076B030CA7AD3CC310E8160AE84B264F981CEFAF6C80EA02B368EAF1A
- Size: 545KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Community Gold Standard Brochure

- Abstract: The Community Gold Standard (CGS) is a comprehensive Information Assurance (IA) framework to develop, operate, and maintain an enterprise security plan. This document is an updated re-release with the new NSA21 format.
- Date: 01/20/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-standards/cgs/community-gold-standard-for-information-assurance.cfm
- Category: IA Guidance > IA Standards > Community Gold Standard
- SHA256: 5B06249AD1AE0793B6B73617DE924413102F5C25098895DEE832381086934B75
- Size: 461KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Reducing the Risk of Vulnerabilities in Unix/Linux-Based Operating Systems

- Abstract: Unix/Linux is a family of operating systems that underpin a large portion of government and commercial servers and infrastructure devices. Due to the prevalence of Unix/Linux systems in public and private infrastructure, and the existence of many exploits and implants that are available, ensure system security by following community best practices and understanding current threats and risks.
- Date: 01/04/2017
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/reducing-the-risk-of-vulnerabilities-in-unix_linux-based-operating-systems.cfm
- Category: IA Advisories
- SHA256: 9A608B6080E95E27C24ABE65B8A29196704BAD07A173E1F26AE0C53C64A9A823
- Size: 222KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

PowerShell: Security Risks and Defenses

- Abstract: This document is in response to the Technical Report “Defending Against the Malicious Use of Admin Tools: Powershell CTR-U-OO802243-16. This paper provides a strategy for hardening, defending, and detecting anomalous and malicious use of administrator tool sets.
- Date: 12/01/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/powershell-security-risks-and-defenses.cfm
- Category: IA Guidance > Security Tips

- SHA256: 45E1F703C357886D200A60243B064295525716E2BD55ABA08A8CED879B52D316
- Size: 277KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Windows 10 for Enterprises

- Abstract: This document describes features present in Windows 10 Enterprise 64-bit that can disrupt exploitation techniques and tools used against national Security Systems today and how the timely adoption of new releases can help to protect systems in the future.
- Date: 12/01/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/windows-10-enterprises.cfm
- Category: IA Guidance > Security Tips
- SHA256: 3FADDEBEBBABE539AA1BE83197B4D23B6B105E40F7706AB884021F9695DE6AA7
- Size: 463KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Long-lived Hashes for Active Directory SmartCard Required Accounts

- Abstract: It is well-known that passwords and their hashes can often be copied and reused by malicious cyber actors. Requiring smartcards or other hard tokens enables stronger authentication because they cannot be copied. Such a token can used by an adversary while the legitimate user is using it if an adversary has compromised the user's device, but not at other times or directly from other devices. When smartcards, are required to login to Windows Active Directory (AD) Domains, a random password is

created and its hash is associated with the account. This allows the device (via the user's account) to use legacy authentication protocols such as NTLM to gain access to resources. In this case, the long random password is better than most user-chosen.

- Date: 11/22/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/long-lived-hashes-for-ad-smartcard-required-accounts.cfm
- Category: IA Advisories
- SHA256: 50C59F19E6F384AC9C744395661C92C5C6152996D25BD9F70437AA15F3A15ED4
- Size: 392KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Eliminating Control Flow Exploitation

- Abstract: Many attacks rely on the ability of an adversary to manipulate the normal, expected flow of the legitimate software executing on a platform. This talk will summarize the mitigations NSA is developing with industry to address this attack vector at a fundamental level and in a way that is largely invisible to the end user and administrator.
- Date: 11/21/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/eliminating-control-flow-exploitation.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: AB3EEF36C47AA6937C72A5F59504BEACDAC1A024F22D005CE121993981332CC4
- Size: 1,558KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Voice and Video over IP

- Abstract: An overview of Video and Voice Over Internet Protocol (VVOIP) will be presented along with security concerns and NSA's recommendations on how to build a secure VoIP architecture.
- Date: 11/21/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/voice-and-video-over-ip.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 43DB1DBAA499413A8F7E6F8ADBE6C8987E77A62D36C23C8FD8F73AC20CD882C0
- Size: 939KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Top Ten IA Mitigations

- Abstract: Learn about how NSA's Top 10 Information Assurance Mitigations obstruct the intrusion lifecycle into networks and have been applied in response to real intrusions in order to mitigate the threat techniques used.
- Date: 11/21/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/top-ten-ia-mitigations.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 5A296EA36EF6A2D05B9B39AD4EC8315D2F3AA9F16E1629C5A6BC96B050488B60
- Size: 1,544KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Overcoming Barriers to Adopting Top 10 IA Mitigations

- Abstract: While fundamental in nature, implementing the Top 10 Information Assurance Mitigations presents challenges, for a variety of reasons. This brief will explore common challenges and suggest potential strategies to overcome them.
- Date: 11/21/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/overcoming-barriers-to-adopting-top10-ia-mitigations.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: D1AEB5A98BA10AD7933C439E9B9592C0AC8DF66C7CE82D309C41925299175E88
- Size: 1,871KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Securely Configuring Adobe Acrobat

- Abstract: Adobe Reader is the predominant PDF reader, one that added numerous security features over the last few years. This talk will highlight the security features in the most current version along with our recommended settings.
- Date: 11/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/securely-configuring-adobe-acrobat.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 2DC76AC9863E66DBFC58EA699FD4D910C18CBC8F08CE68BCF46DA323C7E2AA33
- Size: 1,120KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mitigating Insider Threats

- Abstract: External cyber intrusions can be difficult to defend against. Internal intrusions by insiders are even more difficult to defend against. Learn about mitigations that can be effective against insider threats.
- Date: 11/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/mitigating-insider-threats.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 21EE5E2FCC14DB7CEAEFB0AF24E936C554CCA7CC34ADBFE021ADCADF9EE5A5E1
- Size: 931KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Comply to Connect

- Abstract: Ensuring that devices on a network are not vulnerable is hard to do. Comply to Connect (C2C) simplifies this by enforcing that patches and hardened configuration are applied to devices before they connect and updated continually. Learn about the benefits of C2C and how easily it can be leveraged to improve most networks.
- Date: 11/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/comply-to-connect.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: CAB1F1EE31F4EAD6613ECAA66C13CE38A2577490928A9E11C40836DB349B5FB3
- Size: 1,106KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Whitelisting Best Practices

- Abstract: Cyber defense is not easy. Application Whitelisting is the number one mitigation from the NSA's Information Assurance Top 10, yet many network owners find it a challenge to implement. Learn about some of the common barriers to implementing Application Whitelisting and the best practices for overcoming them. This presentation will be at the Intermediate level.
- Date: 11/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/application-whitelisting-best-practices.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 99A8000927736863332DFD55EB759E32E93915428FB51DBBF8B747C3DCCA7C74
- Size: 1,394KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Algorithms to Support the Evolution of Information Assurance Needs

- Abstract: This document provides background and insight into NSA's intentions for the SIMON & SPECK lightweight block ciphers, and answers frequently asked questions about these designs.
- Date: 11/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/algorithms-support-evolution-ia-needs.cfm
- Category: IA Guidance > IA Solutions For Classified > Algorithm Guidance
- SHA256: 7476BBABA8F029789F7F0FFB30868D87176B1AD7B7E8F41D5081B3EAF2AE99F0
- Size: 119KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Isolation Containment

- Abstract: Given that writing fully secure code remains an elusive goal, other techniques such as isolating processes to limit the adverse effect of a compromise are promising. This talk will summarize some of the techniques, both integrated into the operating system and available as third party add-ons, to provide this isolation.
- Date: 11/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/application-isolation-containment.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 6027A24D701D5D36CC9107FA33DB0B4E54077E9735DA7606A1DD2EA1922EE04D
- Size: 907KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Building the Cyber Workforce Pipeline: Preparing for Today, Tomorrow, and the Day After Tomorrow

- Abstract: An overview of National Cryptologic School's (NCS) programs that are building the cyber workforce pipeline. The College of Cyber's Centers of Academic Excellence in Cybersecurity (CAE-C) programs influence at the collegiate level for tomorrow's workforce. NCS's GenCyber Summer Camps for students and teachers are preparing for the next generation workforce at the K-12 level.
- Date: 11/19/2016

- Link: https://apps.nsa.gov/iaarchive/library/ias/building-national-capacity/building-the-cyber-workforce-pipeline-preparing-for-today-tomorrow-and-the-day-after-tomorrow.cfm
- Category: IA Symposium > Building National Capacity
- SHA256: 875939871FFCA7D28345F501B2694CBD42C88006E7F3C241B58C796D3A40AEE4
- Size: 1,589KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

The NSA Codebreaker Challenge

- Abstract: In this presentation we'll discuss the NSA Codebreaker Challenge, a reverse engineering challenge problem aimed at both strengthening the nations skills in this area while also providing NSA with a new avenue to identify and recruit top talent. We'll talk about our experiences with holding the Codebreaker Challenge over the last three years, discuss the design of both the technical aspects involved and the supporting incentive structures that encouraged participation, and we'll present lessons learned along the way.
- Date: 11/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/building-national-capacity/nsacodebreakerchallenge.cfm
- Category: IA Symposium > Building National Capacity
- SHA256: 7C2E494D3012A14E5FC0A1443646998F9CB5409C84EADA157C491D33C072AEFC
- Size: 817KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Training and Certification:Impacting NSA's Mission

- Abstract: The National Security Agency (NSA) knows that its workforce is the critical component to completing its mission of protecting our nation and its allies. To do this, key workforce functions must be capable of performing each of its tasks at a one hundred percent proficiency. Certifying mission-critical employees requires a comprehensive approach that is customized for each functional position. The critical tasks must be current and use the best learning technologies and management capabilities in the industry.
- Date: 11/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/building-national-capacity/certificationimpact.cfm
- Category: IA Symposium > Building National Capacity
- SHA256: FE8F8DB1E1CCED1590CC4E73413585DFB94B6D4C7E23A63E8C049526A204CC2C
- Size: 1,694KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Joint COMSEC Monitoring Activity Findings and Trends

- Abstract: JCMA frequently discovers critical sensitive network information that could jeopardize US Military and VIP Civilian Leadership tactical intentions including PII data, tactical travel plans, joint force locations of ships and aircraft. This briefing will advise of Top 10 disclosures and mitigation that thwarts the use of the disclosed unclassified information.
- Date: 11/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/defense-at-cyber-speed/jcma-findings-and-trends.cfm
- Category: IA Symposium > Defense At Cyber Speed
- SHA256: 79C5033460B94D56905651C81425451F0F1781EA7BA530BEF7EB77BA3034CB08
- Size: 1,093KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Compliance Training for Technical Professionals: A Case Study

- Abstract: Technical professionals need more than a list of requirements to build internal controls into systems – they need to learn what questions to ask up front to ensure they have the right compliance requirements. Explore the evolution and development of Mission Compliance for Technical Professionals, an online training program designed for individuals that are building privacy compliance into systems, software, tools, and analytics. Learn about the challenge of incorporating Subject Matter Experts appropriate to each of the various technical work roles; training topics and key messages; recognizing and mitigating errors in all phases of the IT lifecycle – building, maintaining, and updating.
- Date: 11/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/building-national-capacity/compliance-training.cfm
- Category: IA Symposium > Building National Capacity
- SHA256: 7215022AE22BD30A4B3957CA1B532BFF94B108C442CB7AC92AD9E5FAAFAAC916
- Size: 2,243KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Third Party Services Your Risk Picture Just Got a Lot More Complex

- Abstract: For some time now, the U.S. Government has sought the best means to protect national security interests without inappropriately undermining the value (i.e., innovation, efficiency) produced by the global information and communications technology

(ICT) supply chain. While past efforts have focused on managing supply chain risk associated with manufactured equipment and software, the new emerging concern is managing the risks associated with outsourced services.

- Date: 11/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/defense-at-cyber-speed/third-party-services-your-risk-picture-just-got-a-lot-more-complex.cfm
- Category: IA Symposium > Defense At Cyber Speed
- SHA256: E70A48E43B01AFD2B6BF0201B926B72C7010F5C7770AA7E5CFE000229014990E
- Size: 864KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Making Mitigations Matter Measuring Host Mitigation State

- Abstract: Mitigations are a significant factor when considering the risks applicable to a network and must be accounted for in order to provide a sense of priority to any additional mitigations that should be applied. This talk will explore means created or under development by NSA to accurately represent the state of mitigations on a network using automated risk scoring systems, with the results tied to the list of mitigations NSA believes are particularly critical. Specific topics include the Splunk Assessment of Mitigation Implementations (SAMI) capability and how mitigations can be covered in vulnerability assessment systems like DISA's Continuous Monitoring and Risk Scoring (CMRS) effort and DHS's Contiguous Diagnostics and Monitoring (CDM) program.
- Date: 11/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ias/adversary-mitigations/t2_making-mitigations-matter.cfm
- Category: IA Symposium > Adversary Mitigations
- SHA256: 961D28FB4A10AFF788BCA78CFD4735E3E4007318699CABC2E33ED03D91094514
- Size: 613KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Defending Against the Malicious Use of Admin Tools: PowerShell

- Abstract: Malicious actors are using our own tools against us. Why reinvent the wheel or drop something new, something distinguishable, when the tools used on every network every day will provide you all you need? This paper provides a strategy for hardening, defending, and detecting anomalous, and malicious, use of administrator toolsets. In particular, this paper will focus on Microsoft's PowerShell and will provide a methodology for hardening and defending it from adversarial use.
- Date: 11/11/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/defending-against-the-malicious-use-of-admin-tools-powershell.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 8EC2924D1DF2E9E698AE2089C028075FD6E2902E3F8F3E00C11395D831EC7A06
- Size: 850KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Blocking Macros from Internet Originated Microsoft Office Files

- Abstract: Microsoft Office files and documents may contain a macro, an embedded program written in Visual Basic for Applications (VBA). Although VBA macros have legitimate uses, macros in Microsoft Office have proven themselves to be a long-lasting and increasingly popular attack vector. In response to this threat, Microsoft has recently provided an ability to block the execution of VBA macros, in files downloaded from the Internet, for Office3 2013 and 2016.
- Date: 11/10/2016

- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/blocking-macros-from-internet-originated-microsoft-office-files.cfm
- Category: IA Advisories
- SHA256: 154AA5CD26BCB59D0B35B80A7A9AABEFD5216DBEA81A813B299806825F75C235
- Size: 189KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Hardening Authentication Update

- Abstract: On many networks, in order for users to be granted access to network resources, a user must prove that he or she is an authorized user. This is the process of user authentication. A user can be authenticated by what he has (e.g. an ID card or token), what he knows (e.g. a PIN or password), or what he is (e.g. biometric data). More robust authentication processes use two or more of these factors, called multi-factor authentication.
- Date: 11/03/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/hardening-authentication-update.cfm
- Category: IA Guidance > Security Tips
- SHA256: 66153221D88CDC59AF94B5EF0CFEA30F9BB696DBAF7DB715EE7DD21339672753
- Size: 319KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Manageable Network Plan Teaser Update

- Abstract: This document is the updated Manageable Network Plan Teaser providing highlights of the Manageable Network Plan.
- Date: 11/02/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/networks/manageable-network-plan-teaser-update.cfm
- Category: IA Guidance > Security Configuration > Networks
- SHA256: 65F46A09BE91C713C31E136724853755DCA9C5FFB029E918689E4D38E7680C18
- Size: 301KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Assess the Mess

- Abstract: This is a technical document/manual for use by DoD, government, and industry ICS owners and operators. It provides methodologies to collect and analyze host and network data on ICS networks in order to baseline and secure these infrastructures.
- Date: 11/01/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/assess-the-mess.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: 7D9941ADED47603940E9670CDD8A13D9B894028AF781A645D2FC5D492AA2DF24
- Size: 3,847KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Linux Kernel Privilege Escalation Vulnerability CVE-2016-5195

- Abstract: On 17 October 2016 CVE-2016-5195 was released, affecting all older Linux kernel versions from 2.6.22 to 4.8.3. This vulnerability affects systems world-wide and is of National concern. This privilege escalation vulnerability allows any unprivileged user, defined as a user with restricted permissions, to gain full root access. The vulnerability is also known by the moniker, Dirty COW, which is derived from Copy of Write.
- Date: 10/27/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/linux-kernel-privilege-escalation-vulnerability-cve-2016-5195.cfm
- Category: IA Advisories
- SHA256: 7DF27B900121C4FC6C285A072E0569655D0E8BB30AA3EF5D6C2AB4C3387F843E
- Size: 275KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Configuration Guide for Browser Updates

- Abstract: Web browsers must be updated on a frequent basis in order to resist highly-scalable, low cost attacks. This document provides a per-browser approach for administrators to keep each major browser updated. Technical details provided in this guide are subject to change as operating systems and browser software evolve, but the overall strategies are likely to remain consistent.
- Date: 10/14/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/security-configuration-guide-for-browser-updates.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: F009EB5B3F17426DF20E2CFD50489AED85F257ADF7A7D09266E2F02370845A75
- Size: 721KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Best Practices for Keeping Your Home Network Secure (Update)

- Abstract: Best Practices for Keeping Your Home Network Secure Factsheet
- Date: 09/28/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/best-practices-for-keeping-your-home-network-secure-updated.cfm
- Category: IA Guidance > Security Tips
- SHA256: AA4E18DBC8EE6FFE857146A9D5F23FE16773BF77DC782D85CD7466CB77B9ACE9
- Size: 341KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Recommendations to Mitigate IKEv1 Vulnerability in Cisco Network Devices

- Abstract: Recommendations to Mitigate IKEv1 Vulnerability in Cisco Network Devices document
- Date: 09/20/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/recommendations-to-mitigate-ikev1-vulnerability-in-cisco-network-devices.cfm
- Category: IA Advisories
- SHA256: 1EECD21B2511DC7E4F3C05E9237E4BE208C93D75A8680B9C026C74A84FB08C98
- Size: 216KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Outdated Network Devices and Unsecure Protocols and Services Expose Network Infrastructure to Compromise

- Abstract: Outdated network devices have known and unknown vulnerabilities that expose the network to severe risk. Unsupported, also called end-of-life, devices and software versions will not receive patches from vendors even for known vulnerabilities. Improperly secured communication protocols and services and insecure credentials increase the risk of unauthorized access and modification to the network infrastructure. When network infrastructure devices are deployed, these devices remain online for several years and are rarely rebooted, patched, or upgraded. Network infrastructure devices include routers, switches, access points, gateways, proxies, firewalls, and others. Common improperly secured protocols are Simple Network Management Protocol (SNMP), Secure Shell (SSH), Telnet, and others. Networks must not use vulnerable devices and software versions or unsecured protocols unless absolutely necessary, and, if necessary, ONLY along with supplemental mitigations to detect and prevent compromise and lateral movement.
- Date: 09/02/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/outdated-network-devices-and-unsecure-protocols-and-services.cfm
- Category: IA Advisories
- SHA256: 5DBEC3809884EC3E5CD7841050E3C7B018FCA8AAD649CFAC63D227C61633F9DE
- Size: 893KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Vulnerabilities in Cisco Adaptive Security Appliances Identified in Open-Source – Version 1

- Abstract: On 15 August 2016, exploits targeting vulnerabilities previously not publicly known in Cisco Adaptive Security Appliances and other security devices were released on the Internet. On 17 August 2016, Cisco published an advisory (cisco-sa-20160817-asa-snmp) and released a patch for a vulnerability in its ASA devices, determined to be an SNMP Remote Code Execution Vulnerability, due to a buffer overflow.
- Date: 08/20/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/vulnerability-in-cisco-adaptive-security-appliances-identified-in-open-source-v1.cfm
- Category: IA Advisories
- SHA256: 7EF98A2E0F4AAF1FBF1437C06BD7EF46311406BDD8006211799DDDF82F185040
- Size: 196KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Bluetooth for Unclassified Use: A Risk Discussion for IT Decision Makers

- Abstract: Bluetooth is a short-range wireless technology found in many commercial devices used for computing, communication, and healthcare. The decision to add Bluetooth devices to an IT landscape must be based on well-informed consideration of the risks and benefits. Different types and implementations of Bluetooth devices may incur varying levels of risk, so a good Bluetooth policy likely lies somewhere between permitting all and prohibiting all Bluetooth devices. This document provides information about the operation of Bluetooth and the threats against it, and suggests questions that decision-makers can ask in order to identify the devices most likely to behave in accordance with a secure Bluetooth policy.
- Date: 08/04/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/bluetooth-for-unclassified-use_a-risk-discussion-for-it-decision-makers.cfm
- Category: IA Guidance > Technical Briefs

- SHA256: F0BE2479934EE6C9F4B6D24012B7E1D95A9CA5241107B8D93F6FF14003FF8CCA
- Size: 348KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Bluetooth for Unclassified Use: Guidelines for Users

- Abstract: Bluetooth is a short-range wireless technology found in many commercial devices used for computing, communication, and healthcare. Bluetooth offers the convenience of low-power wireless device-to-device communication, opening the door for diverse and exciting use cases for recreation and business. As with other technologies, threats exist today that endanger the integrity, confidentiality, and availability of the information transferred to and from devices using Bluetooth. This document provides background on Bluetooth functionality and includes recommendations for using Bluetooth securely to mitigate possible risks.
- Date: 08/04/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/bluetooth-for-unclassified-use_guidelines-for-users.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 32F40FB74577D04032FF55653119D37441BA5E5A9128A246A5284CBCA05FA2B0
- Size: 313KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Bluetooth for Unclassified Use: Guidelines for Developers

- Abstract: Bluetooth offers the convenience of low-power wireless device-to-device communication, opening the door for diverse and exciting use cases for recreational and business users. The proliferation of Bluetooth into a broad range of modern personal devices has generated a demand for software applications that enable users to interact with it. As with other technologies, threats exist today that endanger the integrity, confidentiality, and availability of the information transferred to and from devices using Bluetooth. The design of any software involved in transferring data via Bluetooth should include measures to protect the user's device and data. This document provides background on Bluetooth functionality and recommendations for developing secure Bluetooth applications.
- Date: 08/04/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/bluetooth-for-unclassified-use_guidelines-for-developers.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 3193DD7ACC7B435DB21380D31CE7E9C005068B5523A4C54AC32FD731CD4A158C
- Size: 340KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Take Advantage of Software Improvement

- Abstract: New security technologies and software development methodologies have drastically improved the security posture of software and systems released over the last decade. Specifically, new software antiexploitation features in conjunction with the adoption of systematic development processes have contributed to this improvement. Obtaining value from software improvements is only possible through product upgrades and timely deployment of patches.
- Date: 08/03/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/take-advantage-of-software-improvement.cfm
- Category: IA Guidance > Security Tips
- SHA256: F8355E80378E6E2F92CCB07C349293191F3A8AE51692FF81BA2A40CF6933B629

- Size: 329KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Implementing a Secure Administrator Workstation Using Device Guard

- Abstract: Defenders must raise the cost for an adversary to obtain high-value domain credentials after an initial intrusion. One such way is through a dedicated administrator workstation for performing highly-privileged tasks subsequently referred to as a Secure Administrator Workstation (SAW). SAWs address credential theft techniques by limiting highly-privileged credentials to specific hardened systems. This guide will help DoD administrators configure a hardened admin workstation using Windows 10 and Device Guard.
- Date: 07/27/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/windows-10-device-guard.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: A2A83354BA9120EC2F3892CE8FD9C2A2D672DD37F0CD5B02CE8EC63F6EE06F8D
- Size: 957KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Outdated Software and Protocols Updated

- Abstract: Outdated and unsupported software and protocols have known and unknown vulnerabilities that expose the network to severe risk. Older software versions were not developed with modern secure coding practices and do not incorporate the most recent mitigations designed to prevent and contain intrusions.

- Date: 07/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/outdated-software-and-protocols-update.cfm
- Category: IA Advisories
- SHA256: 48F933C244AB102F006E115B8FD3D0F3D61831A19A3A2F16DFE83FA3FF153624
- Size: 448KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Recommendations to Mitigate Unauthorized Cisco ROMMON Access and Validate Boot ROMs

- Abstract: New attack methods have been observed targeting networking devices running Cisco Internetwork Operating System (IOS) Classic platforms. Adversaries access the device with valid administrative credentials and then upload malicious code. Compromised devices are used to establish persistence and manipulate device behavior. Refer to the Cisco Security Activity Bulletin for additional threat information. This Information Assurance Advisory includes recommendations and procedures to identify the loaded ROM image and recover with a trusted ROM image, improving assurance in the device.
- Date: 07/15/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/recommendations-to-mitigate-unauthorized-cisco-rommon-access-and-validate-boot-roms.cfm
- Category: IA Advisories
- SHA256: BA1BC155A943A6404F097F8176EB2300773AB67F6754A6CED04C65E6551F3365
- Size: 160KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Filter Sidecar Protocol (FSP) Specification

- Abstract: The purpose of this document is to describe the cross domain solution (CDS) Filter Sidecar Protocol (FSP). A filter sidecar is generally considered to be a network connected system, usually on a trusted operating system, that provides high assurance content inspection and sanitization functions for Cross Domain Solutions. The Filter Sidecar Protocol is intended to provide a mechanism for making new filtering capabilities available to an existing cross domain solution by adding a certified sidecar platform. As long as the CDS is tested to properly implement the Filter Sidecar Protocol, users should be able to add new content types without having to completely recertify the CDS since the filter sidecar would be separately certified.
- Date: 07/07/2016
- Link: https://apps.nsa.gov/iaarchive/library/reports/filter_sidecar_protocol_spec_v1_0_6-20171212.cfm
- Category: Reports
- SHA256: 2DB650174AB073705D518AFE7D7CEBB72F42F64EF215FAA5FF75FC1653AD1B8C
- Size: 822KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Network Mitigations Package-Infrastructure

- Abstract: The security community continues to address emerging network threats. The new security model now consists of prevention, detection, containment, and response to mitigate threats. The Network Mitigations Package-Infrastructure (NMP-I) focuses on layering information system network defenses enabling communications while controlling adversaries' ability to move laterally through the network. The NPM-I provides guidance to aid organizations as well as system administrators in hardening core network infrastructure to protect network infrastructure access, network availability, and critical information.
- Date: 06/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/network-mitigations-package-infrastructure.cfm

- Category: IA Guidance > Security Tips
- SHA256: 50BE84C7A0CAB53E5F1386F1B7C9547B059E20BC61E07A1D210659A2B2322D11
- Size: 1,010KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Perform Out-of-Band Network Management

- Abstract: Out-of-Band (OoB) network management is a concept that utilizes an alternate communication path to remotely manage network infrastructure. These alternate channels are designed and implemented to isolate management traffic from normal user traffic, so compromised user devices and communications cannot affect network operations or compromised network devices.
- Date: 06/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/perform-out-of-band-network-management.cfm
- Category: IA Guidance > Security Tips
- SHA256: 1C46633A5616CC67165233BECD6AC0A8AE23AD7A0EB7A2448FDE8C10C1627A14
- Size: 493KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Validate Integrity of Hardware and Software

- Abstract: Grey market devices are network infrastructure devices acquired through unofficial channels. These devices can cause a loss of intellectual property and damage to reputation. Counterfeit hardware and software have appeared across many industries.

They are often introduced into the supply chain through non-reputable re-sellers. Unknowingly using grey market devices can significantly comprise your network by introducing vulnerabilities such as logic bombs, back doors, and altered security functions. It is important to confirm the integrity of devices and software throughout the entire supply chain.

- Date: 06/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/validate-integrity-of-hardware-and-software.cfm
- Category: IA Guidance > Security Tips
- SHA256: 69EF0B09E524A26C82613CA5ED876B8976F02A64F1330838A2674B1E0400E688
- Size: 621KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Harden Network Devices

- Abstract: There are several ways to access network devices: through an administration connection, console line, auxiliary line, and virtual terminal connection. Each method to access network devices should be secured to prevent any unauthorized access to the network device.
- Date: 06/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/harden-network-devices.cfm
- Category: IA Guidance > Security Tips
- SHA256: 0DD459107C40F0120A4852AAC8FD97DAD9EA8EBD4B5817E522BCA0A92B8CF7F3
- Size: 459KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Secure Access to Infrastructure Devices

- Abstract: Secure access enables an administrator to maintain positive control of user accessing network infrastructure. There are multiple secure access devices and techniques that are scalable and can be used to keep your networks secure depending on which method fits the requirement.
- Date: 06/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/secure-access-to-infrastructure-devices.cfm
- Category: IA Guidance > Security Tips
- SHA256: 77B96DA10FE641B9017EB2AE3050D6C11B32ECE8CB9DD168507A11971530FCF9
- Size: 496KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program Vulnerability Assessment Accreditation Scoresheet 1.0

- Abstract: This is the VA Score Sheet used during NSCAP accreditation evaluations
- Date: 06/08/2016
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/assets/public/nscap-va-accreditation-scoresheet-v1.cfm
- Category: Supporting Documents > Assets > Public
- SHA256: 36D7A3AA8D2634BBA93CCA8EE1A93FCA3D1E1A8481EEDAB26413ACC54F958BB6
- Size: 56KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Protecting Virtual Private Network Traffic 2016

- Abstract: In March 2015 IAD released the Information Assurance Advisory (IAA) “Protecting Virtual Private Network (VPN) Traffic”. That advisory recommended utilizing a key size of 4096 bits or DH group 16. Since the release of that IAA, IAD released an advisory memo. To maintain consistency this IAA updates the previous one and includes the new guidance of a minimum key size of 3072.
- Date: 06/07/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/iaa-protecting-vpn-traffic-2016-unclassified.cfm
- Category: IA Advisories
- SHA256: FC208B84F6AEA24E69ACB1CFE758D5A6EF97CEC4AB1BB5ED1312826A7A3F84F6
- Size: 416KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Guidelines for ConfigurationPatch Management in Industrial Control Systems

- Abstract: This document was written with contributions from Subject Matter Experts at the Department of Homeland Security (DHS) and the National Security Agency (NSA). This document serves as an appendix to “Seven Strategies to Defend Industrial Control Systems”. Application Whitelisting (AWL) can detect and prevent attempted exectution of malware uploaded by adversaries. The static nature of some industrial control systems (ICS) computers, such as database servers and human-machine interfaces, makes these ideal candidates to run AWL. In some situations deploying AWL on ICS computers is simple, but it can be challenging in others. Operators are thus encouraged to work with vendors to baseline and calibrate AWL deployments.
- Date: 05/20/2016

- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/guidelines-for-configuration-and-patch-management-in-industrial-control-systems.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 01CA1AED067F0627D12E6AD815741F3178EB7F569ED61E7ACF58BDB8B537C90B
- Size: 1,663KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

ImageMagick Remote Code Execution Vulnerability CVE-2016-3714

- Abstract: This document describes a remote code execution vulnerability in earlier versions of ImageMagick, a versatile cross-platform image processing tool, and describes the mitigation actions to take.
- Date: 05/19/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/imagemagick-remote-code-execution.cfm
- Category: IA Advisories
- SHA256: 7D7CC58E2C19E06BE769DAC866B4E4C8DF487DEA876C29BC028EE6D5D7DCB7A3
- Size: 277KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Information Assurance Advisory Information Sheet

- Abstract: This document defines the purpose of an Information Assurance Advisory (IAA) and the reason for its use.

- Date: 05/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/information-assurance-advisory-information-sheet.cfm
- Category: IA Guidance > Security Tips
- SHA256: 9EA2994F1E07E84BCC70515C7E7FFFACC1F72552C915D637FE0C15D4215510AF
- Size: 369KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Apple Quicktime Reaches End-of-Life for Windows Factsheet

- Abstract: Apple has officially ended support for QuickTime on Microsoft Windows. In January of 2016, Apple released the final update of QuickTime for Windows and removed the QuickTime plugin from browsers to help mitigate future vulnerabilities. In April of 2016, two new vulnerabilities were released, ZDI-16-241 and ZDI-16-242, that affect the most recent version of QuickTime for Windows. The vulnerabilities allow an attacker to remotely exploit a system by sending the victim a malicious .MOV file that is then viewed with QuickTime. Because Apple has ended support, Apple will no longer be deploying patches or future releases on Windows leaving the software unpatched. Windows systems running QuickTime are vulnerable until the software is removed. Apple and QuickTime are registered trademarks of Apple, Inc. and Microsoft and Windows are registered trademarks of Microsoft Corp.
- Date: 05/09/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/iaa-apple-quicktime-reaches-end-of-life-for-windows.cfm
- Category: IA Guidance > Security Tips
- SHA256: A896C06B83356E0813DB559BE90A193A00BA60CC4A79C5AB9413C060508EB83C
- Size: 194KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program Cyber Incident Response Assistance Accreditation Instruction Manual 3.2

- Abstract: CIRA instruction manual used during NSCAP accreditation evaluations.
- Date: 05/04/2016
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/cira-accreditation-instruction-manual.cfm
- Category: Supporting Documents
- SHA256: 94270066BDAABB48A5D77A366A1189C4530374290673AA2390F8022B142FD3C9
- Size: 2,527KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program VAS Accreditation Instruction Manual

- Abstract: The purpose of this document is to provide application instructions and accreditation guidelines to organizations interested in applying for and receiving this accreditation. This accreditation is associated with two general VA activities: Certification and Accreditation (C&A), including C&A renewals, and Security Posture Assessments.
- Date: 05/02/2016
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/nscap-vas-accreditation-instruction-manual.cfm
- Category: Supporting Documents
- SHA256: 42CA8FD920726DA7F1B25A43270CD109C91EB931FFDAC35ECBD0D66DFBFD5038
- Size: 1,343KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Wireless Intrusion Detection System Technical Brief

- Abstract: This document describes current capabilities and limitations of commercial Wireless Intrusion Detection Systems (WIDS). It includes the general types of attacks that WIDS can and cannot detect.
- Date: 04/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/wids_tech_brief.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: F47010A478C53E22E1DC98929324791B4A4AC642D603D435EB8DD8BF7EE4BE29
- Size: 307KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Ransomware - Locky

- Abstract: Malware placemats summarize a particular piece of malware based on researched, collected and fused information and analysis. Placemats are intended to inform customers of the past, present, and potential future infections, characteristics, and best practices/mitigations on particular pieces of malware. They are also meant to be eye-catching and easy to digest reports for decision makers and cyber defense practitioners. This placemat focuses on the ransomware Locky. Locky's infection rate accounts for a large portion of the ransomware infections currently seen across industry.
- Date: 04/11/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/ransomware-locky.cfm

- Category: IA Guidance > Technical Briefs
- SHA256: 5ADDBFD4DA2E0CC3606B570DBC47A79946681E2115C811FBE1DA5402F222E7BB
- Size: 418KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Guidelines for Application Whitelisting Industrial Control Systems

- Abstract: This document serves as an appendix to the “Seven Steps to Defend Industrial Control Systems” document, providing additional conceptual-level guidance on implementing application whitelisting. Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some industrial control system (ICS) components, such as database servers and human-machine interfaces, makes these ideal candidates to run AWL. Operators are thus encouraged to work with vendors to baseline and calibrate AWL deployments.
- Date: 04/01/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/guidelines-for-application-whitelisting-industrial-control-systems.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: 6E69708A77F5F44B9BEA68E9C2F5ACEC8D96A41803CEF2A27F2FB4543A5AC610
- Size: 1,065KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Joint Information Environment

- Abstract: NSA is the Security Advisor for the development of the Joint Information Environment (JIE) cyber security architecture. This document provides an overview of the JIE development process and Cyber Security Reference Architecture (CS RA) security framework.
- Date: 03/16/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/secure-architecture/joint-information-environment.cfm
- Category: IA Guidance > Secure Architecture
- SHA256: 3ACF7EF4E4FFCAECAB82E0C106684A7BC4E805D9432AF1CEA69E0765CB562C97
- Size: 600KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Information Assurance Top 9 Architectural Tenets

- Abstract: This document describes the top 9 Information Assurance Architectural Tenets to address cyber threats and reduce the frequency and impact of incidents.
- Date: 03/16/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/secure-architecture/ia-top-9-architectural-tenets.cfm
- Category: IA Guidance > Secure Architecture
- SHA256: 1CA290C533FCF7F53E0A9555ECACEBAF8329467D2EFF99062DAC83CA45D7F532
- Size: 308KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Trusted Engineering Solutions

- Abstract: Trusted Engineering Solutions (TES) incorporates security engineering and architecture solutions, to provide the next generation in cybersecurity.
- Date: 03/15/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/secure-architecture/trusted-engineering-solutions.cfm
- Category: IA Guidance > Secure Architecture
- SHA256: 588AC45A2F8E63A0C1F3D7E663A5FF67E52F335F8FB4EA1192ADCCC055EBA2B5
- Size: 739KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Highlights of Windows 10

- Abstract: This document provides a high-level description of new security features in Windows 10 for senior technology leaders. It describes how these features disrupt attacker tools, techniques, and procedures used against National Security Systems today.
- Date: 02/24/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/security-highlights-of-windows-10.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: 06869882C4B00A0F0B08433810CCEEB3DB20CDC8965786313F3FB3148D2B9F7B
- Size: 664KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Network Device Integrity -NDI- Methodology

- Abstract: The Network Device Integrity (NDI) Methodology attempts to answer “How do I know if my network device has been compromised?”, and provides methods for detecting unauthorized access, software modifications, and hardware modifications
- Date: 02/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/reports/network-device-integrity-methodology.cfm
- Category: Reports
- SHA256: CCF09EEC22673602CF7EEBE68F150531318F7363E4303A97B07767669837DD90
- Size: 231KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Network Device Integrity on Cisco IOS Devices

- Abstract: This document describes how to perform the Network Device Integrity (NDI) Methodology specifically on Cisco IOS systems.
- Date: 02/23/2016
- Link: https://apps.nsa.gov/iaarchive/library/reports/network-device-integrity-ndi-cisco-ios-devices.cfm
- Category: Reports
- SHA256: C493EECFC5F42BB857837CEC61D76E9A8DF2221A4F258115B07C59F5DD2F24B9
- Size: 361KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

IAD's Top 10 Information Assurance Mitigation Strategies

- Abstract: Fundamental aspects of network security involve protection, detection and response measures. This provides guidance for organizations to secure and manage networks thus making the networks defensible and recommends proactive mitigation advise to counter cyber threats.
- Date: 02/18/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm
- Category: IA Guidance
- SHA256: DCA3B517BEEF02981091FC1E80E0D743A542952768A545BA73A2D0953919E8D8
- Size: 463KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Position Zero: Integrity Checking Windows-Based ICS/SCADA Systems

- Abstract: This document outlines several techniques that utilize functionality available within the Microsoft Windows operating system to establish an operational foundation ('position zero') of ICS/SCADA servers and workstations.
- Date: 02/09/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/position-zero-integrity-checking-windows-based-ics-scada-systems.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: 9BA6A0870F39D2EBFE7C16BBCF7BE09D9986CC03FC1FDD0C491F59F826101208
- Size: 3,563KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

2016 IAD's Top Challenges and Efforts

- Abstract: This document presents the top IA technology challenges and efforts in 2016.
- Date: 01/29/2016
- Link: https://apps.nsa.gov/iaarchive/library/reports/iad-top-challenges-and-efforts-2016.cfm
- Category: Reports
- SHA256: 764332CC4C5EFA276BA0D1B2050BE52F9DE04578D15A416D7561C9CBDC96A688
- Size: 659KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Journal of Information Warfare, Vol. 14 Issue 2

- Abstract: Once again, Peregrine is collaborating with the NSA on a new special edition of the Journal of Information Warfare (JIW). In this publication, we bring you 9 articles from subject matter experts at NSA, all of which focus on cyber-security efforts that attempt to realize their theme of Confidence in Cyberspace.
- Date: 01/14/2016
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/journal-of-information-warfare-14-2.cfm
- Category: Supporting Documents
- SHA256: 531107745DD175479026BC9DF70BB3F89DBF75523AF1A8A4F443BB9684E5A827
- Size: 2,868KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Commercial National Security Algorithm Suite and Quantum Computing FAQ

- Abstract: This document provides answers to commonly asked questions regarding the Commercial National Security Algorithm (CNSA) Suite, Quantum Computing and CNSS Advisory Memorandum 02-15.
- Date: 01/06/2016
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm
- Category: IA Guidance > IA Solutions For Classified > Algorithm Guidance
- SHA256: CE6618AB88C10ADEA1938E672F8BCF176EA75B96D56AA1825373E250F8DAC2C5
- Size: 253KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

IAD Top Ten Mitigations Questions and Answers

- Abstract: This document answers the eight most commonly asked questions regarding IAD's Top Ten Mitigations. It also provides links to additional information resources and depicts the Intrusion Lifecycle and Mitigations.
- Date: 01/02/2016
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/faq/iad-top-10-mitigations-qa.cfm
- Category: Supporting Documents > FAQ

- SHA256: BA18C8393112B46F470246C6413B6A815716D98867135FBD90CA431051E58BD5
- Size: 504KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Commercial National Security Algorithm Suite Factsheet

- Abstract: Rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms are vital tools that contribute to our national security and help address the need for secure, interoperable communications. This document highlights how the Commercial National Security Algorithm (CNSA) Suite addresses these issues.
- Date: 12/31/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/commercial-national-security-algorithm-suite-factsheet.cfm
- Category: IA Guidance > IA Solutions For Classified > Algorithm Guidance
- SHA256: F2306D49C4822AE2A5D181526CCCBA2E8E080FB9563A037D21CE40EA219E7964
- Size: 344KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Seven Steps to Effectively Defend Industrial Control Systems

- Abstract: Securing Industrial Control Systems (ICSs) against the modern threat requires well-planned and well-implemented strategies. This paper presents seven steps that can be implemented today to counter common exploitable weaknesses in “as-built”

control systems.

- Date: 12/24/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/seven-steps-to-effectively-defend-ics.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: 90ED54DFCA1B7856398F33B3D4DF2DA70B73D94E0B598F3ABB019EE93A74D108
- Size: 1,383KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Recommendations for Configuring Adobe Acrobat Reader DC in a Windows Environment

- Abstract: This document provides guidance on configuring Adobe Reader DC in a Windows environment. Adobe Reader DC is the latest version of Adobe Reader and replaces Adobe Reader XI. The “DC” in the title stands for “Document Cloud” which refers to the cloud based features introduced in Adobe Reader DC.
- Date: 12/02/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/recommendations-for-configuring-adobe-acrobat-reader-dc-in-a-windows-environment.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: 56F25F7AEB8802DB455F28829F2E1D59F804B0648D34CCB26073D1B5AAF6E8FA
- Size: 506KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Manageable Network Plan Guide

- Abstract: A Manageable Network Plan is a series of milestones that can take an unmanageable, insecure network and make it more defensible, more secure and more manageable. Because the plan is intended to be a long-term solution, implementing milestones may require additional resources and time. Once manageable, your network can be secured more efficiently and effectively.
- Date: 12/01/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/networks/manageable-network-plan.cfm
- Category: IA Guidance > Security Configuration > Networks
- SHA256: 11F067F6131AA9DDF11D1D80C4E05345798231F4679B85964532BDCA8F88CD9E
- Size: 5,533KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

IAD's Top 10 Information Assurance Mitigation Strategies

- Abstract: Provides guidance for organizations to secure and manage networks, thus making the networks defensible, and recommends proactive mitigation advice to counter cyber threats.
- Date: 11/25/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/iad-top-10-information-assurance-mitigation-strategies.cfm
- Category: IA Guidance > Security Tips
- SHA256: 339B882DFE9A2C50D3BF23A8D6CC19B194A90E2380C5D39A9E28FE50CE19E795
- Size: 331KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

IAD Best Practices for Securing Wireless Devices and Networks in National Security Systems

- Abstract: IAD has developed a set of best practices for establishing, operating, and using wireless communications devices, either as a component of, or in close proximity to, NSS networks. By implementing the outlined measures, network owners and operators will be better positioned to optimize security, manage risk, and implement vulnerabilities.
- Date: 10/24/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/securing-wireless-devices-and-networks.cfm
- Category: Reports
- SHA256: EB7133497D6C5960BD6F1E47019BD269A445FA874AE2AE82A8157BFF8C54CD31
- Size: 989KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Community Gold Standard 1.1.1 files

- Abstract: Community Gold Standard (CGS) v.1.1.1 files
- Date: 10/22/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-standards/cgs/community-gold-standard-zip.cfm
- Category: IA Guidance > IA Standards > Community Gold Standard
- SHA256: 43C18A2B92C045C10E76DB5A0A6D389022C049E35BD4A81BA21AB49A2A700EC6
- Size: 25,692KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Securing Assets Within a Closed Industrial Control System Network

- Abstract: The second in a series, this document focuses on system security within a “closed” ICS perimeter. It provides a systematic approach for implementing the access control concept of Least Privilege.
- Date: 10/02/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/securing-assets-within-closed-ics-network-perimeter.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: F46C884729B9F73CF259D36F7F3BE253F3D77FC0E3CF5D2C6A655E04A721437E
- Size: 1,354KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Securely Managing Industrial Control System Networks

- Abstract: The fourth in a series, this document focuses on implementing a secure ICS network management program through comprehensive network management policies and procedures. An effective network management program is an essential element of maintaining the security posture of critical ICS networks.
- Date: 10/01/2015

- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/securely-managing-ics-networks.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: F91E42312D54C53319ABA4E13ED9631C2B899C8D358405033A04BB604CA1172D
- Size: 198KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cyber Defense Exercise Winners

- Abstract: This document lists the past winners of the Cyber Defense Exercise (CDX), an annual competition designed to sharpen the skills of our nation’s next generation of cyber warriors.
- Date: 09/23/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/cdx-winners.cfm
- Category: Supporting Documents
- SHA256: 4CF890406AEE299F9C26ACA866A9A00FAD5312BEBF4C789BD17FE6D450D7F5E5
- Size: 141KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Microsoft’s Enhanced Mitigation Experience Toolkit: A Rationale for Enabling Modern Anti-Exploritation Mitigations in Windows

- Abstract: Microsoft's Enhanced Mitigation Experience Toolkit (EMET) is an enhancement to the Windows operating system that stops broad classes of malware from executing. EMET implements a set of anti-exploitation mitigations that prevent the successful exploitation of memory corruption vulnerabilities in software, including many zero-day and buffer overflow attacks.
- Date: 09/16/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/microsofts-emet-a-rationale-for-enabling-modern-2.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: 1D0A10F5C35908D01A16F1A39E8491421043CBEE931D59706C1DC0045CB86C29
- Size: 1,275KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program Frequently Asked Questions

- Abstract: NSCAP_FAQs_Updated-Version_wDisclaimer_02092017
- Date: 09/16/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/faq/nscap-faqs.cfm
- Category: Supporting Documents > FAQ
- SHA256: E3AC6CBFC22BA3684EEC1FF5C045FEF3821FBED5539DB18E033DE82677FCDDAA
- Size: 833KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Scripting for Bash Vulnerability/Shellshock

- Abstract: Security researchers, vendors, and other reporting organizations have commented on the GNU Bash (Bourne Again shell) vulnerability, the severity of the vulnerability, and the critical need to patch vulnerable versions of Bash. Central to their message is the need to test for the vulnerability by issuing the exploit, and then patching the affected systems. This technical report presents an introduction for technical and non-technical managers who are unfamiliar with the Bash vulnerability. In particular, this note introduces a few sample code fragments that can test for the vulnerability without exploiting the vulnerability.
- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/scripting-for-bash-vulnerability-shellshock.cfm
- Category: Reports
- SHA256: 99C1174E894EBACCC9884038F347398FD91B064C60F7B34201614EC26870F5F4
- Size: 665KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Microsoft's Enhanced Mitigation Experience Toolkit Guide

- Abstract: Anti-exploitation mitigations like EMET are increasing in importance. By specifically restricting access to broad classes of exploits, EMET protects software from memory corruption attacks used by many APT actors, protects software in between patch cycles, and protects legacy software even without access to the source code.
- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/microsoft-enhanced-mitigation-experience-toolkit-a.cfm
- Category: Reports
- SHA256: 07E804BA9FABCE06FAC0649B64733F5C6F39C6462C4BE03B8E84DA28B430EDAD
- Size: 1,488KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Host Mitigation Package

- Abstract: Host Mitigations Package (HMP) is designed to aid organizations and system administrators in hardening their host systems.
- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/host-mitigation-package.cfm
- Category: Reports
- SHA256: BA098FD3774DD98FC45E4948213F32580DEA0C751885002AC7541CB8AD41B499
- Size: 1,288KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Highlights of Windows 7

- Abstract: This guide highlights many of the new security features in Windows 7, just one of the many commercial operating systems available.
- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/security-highlights-of-windows-7.cfm
- Category: Reports
- SHA256: 2F6C108733A3A5E95E1EA7D17A1A9D821C1902CBD57DC3EF381DEFF7AD740364

- Size: 412KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Whitelisting using Software Restriction Policies

- Abstract: Software Restriction Policies (SRP) enables administrators to control which applications are allowed to run on Microsoft Windows. SRP is a feature of Windows XP and later operating systems. It can be configured as a local computer policy or as domain policy using Group Policy with Windows Server 2003 domains and later. Using this guide, administrators can configure SRP to prevent all applications in their domain from running except applications they explicitly allow. Utilizing SRP as an application whitelisting technique significantly increases the security posture of the domain by preventing many malicious programs from executing.
- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/application-whitelisting-using-srp.cfm
- Category: Reports
- SHA256: 3194220BFBF72D090512A55194F3FEA5927A914D2F2969A631482EB4A8F418B5
- Size: 385KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Content Automation Protocol Content for Apple iOS 5 Security Configuration Recommendations

- Abstract: These are zip files that go with the Apple iOS configuration guide

- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/associated-scap-content-for-apple-ios-5.cfm
- Category: Reports
- SHA256: E662913C4450085E0F2C0164DB7C561B7B711C33B177ECFA812B795B899860CF
- Size: 29KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Recommendations for Configuring Adobe Acrobat Reader XI in a Windows Environment

- Abstract: This document includes information for using Adobe's Customization Wizard (CW) or Microsoft's PowerShell to configure the necessary settings for uniform distribution of the software throughout an enterprise or on a standalone system. Appendix A lists all of the ARXI security-related settings with recommendations for the environments that should configure those settings.
- Date: 09/15/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/recommendations-for-configuring-adobe-acrobat-reader-xi-in-a.cfm
- Category: Reports
- SHA256: EE255022F471D504707C704E7E4B93C5CA72AD5D54F49F5352F650BCA163B3DC
- Size: 330KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Reducing the Effectiveness of Pass-the-Hash

- Abstract: This document discusses mitigations administrators can deploy, in the interim, to reduce PtH's effectiveness by addressing some of the properties it depends upon.
- Date: 09/14/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/reducing-the-effectiveness-of-pass-the-hash.cfm
- Category: Reports
- SHA256: 2BB4F682A2C48485E332FC0A2FA9E4DDD00B8520424670EF9F588986779ED51A
- Size: 350KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Spotting the Adversary with Windows Event Log Monitoring

- Abstract: This paper focuses on using the built-in tools already available in the Microsoft Windows operating system (OS). Central event log collection requires a Windows Server operating system version 2003 R2 or above. Many commercially available tools exist for central event log collection. Using a Windows Server 2008 R2 or above server version is recommended. There are no additional licensing costs for using the event log collection feature. The cost of using this feature is based on the amount of additional storage hardware needed to support the amount of log data collected. This factor is dependent on the number of workstations within the local log collection network.
- Date: 09/14/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
- Category: Reports
- SHA256: E7FF70328E660A05F0BE079DB72AEBA04AF5769E4856FFD34FBD1EFF77EFA95B
- Size: 871KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Defense in Depth

- Abstract: This paper provides an overview of the major elements of the strategy and provides links to resources that provide additional insight.
- Date: 09/14/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/defense-in-depth.cfm
- Category: Reports
- SHA256: C7DE6ACB92CBFFCF387AE9F055CE5F54C178F51A2FC6F58F74DF73C44534E9E0
- Size: 670KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

NSA Methodology for Adversary Obstruction

- Abstract: This document describes the mitigations needed to pre-posture defensive capabilities and response processes in order to prevent and contain the security of a network.
- Date: 08/05/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/nsa-methodology-for-adversary-obstruction.cfm
- Category: Reports
- SHA256: 5FF75FAFFCCE6AC910D87253C5D47B13444449C71B31FA345C43C507CFFCB07D
- Size: 741KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Adobe ColdFusion Guidance

- Abstract: Adobe ColdFusion has major vulnerabilities. These vulnerabilities enable an adversary to exploit the weakness and potentially gain and expand a foothold onto the owner's network.
- Date: 07/01/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/adobe-coldfusion-guidance.cfm
- Category: Reports
- SHA256: BD68206364094C1DDC7CCD5A741CB97B3E876AAE771C5102EB7487BF45BE689A
- Size: 627KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Virtual Private Network Registration Form

- Abstract: This document is the registration form for VPN.
- Date: 06/01/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/forms-templates/csfc-vpn-registration-form.cfm
- Category: Supporting Documents > Forms Templates
- SHA256: 55D5B36E7A53AD5696EE167766C716A8B4A313DDF9F2CC5000148DE99595FCFB
- Size: 1,017KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Campus Wireless Local Area Network Registration Form

- Abstract: This document is the registration form for Campus WLAN.
- Date: 06/01/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/forms-templates/csfc-campus-wlan-registration-form.cfm
- Category: Supporting Documents > Forms Templates
- SHA256: B5B2C02A27092AB4AE1E1F13586445852EBAF2785DD3C027DF7F5BB2378B4C7F
- Size: 1,017KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

2014 Supplemental Guide to the National Manager's Letter

- Abstract: National Security Directive 42 (NSD-42) and Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Infomation) mandates the National Manager develop effective technical safeguarding policies and standards that address the safeguarding of information within NSS and assess the overall security posture of NSS.
- Date: 05/20/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-standards/cgs/supplemental-guide-to-the-national-managers-letter.cfm
- Category: IA Guidance > IA Standards > Community Gold Standard

- SHA256: CE52C6307F8E855A7FE9A8F33BF9C09565BC93C354E0850B0EBF38DA9B0C2451
- Size: 687KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Frank B. Rowlett Awards Program

- Abstract: Rowlett-Award_Booklet_2016
- Date: 03/31/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/frank-b-rowlett-awards-program.cfm
- Category: Supporting Documents
- SHA256: 489C1D93089A884BB2309A20940A4F9B008CEDF535F3218AA33E036BAB5785AD
- Size: 56KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Apply for Cyber Incident Response Assistance Accreditation Using the National Security Cyber Assistance Program Accreditation Portal

- Abstract: Instructions on how to access the NSCAP Accreditation Portal (NAP).
- Date: 03/17/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/apply-for-cira-accreditation-using-the-nscap-accreditation.cfm
- Category: Supporting Documents

- SHA256: 7AD67952F6C70780FB20A371EB6C37D16A22558F87158CD47BBD52A1D8E0946B
- Size: 234KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

2015 IAD's Top Technology Challenges

- Abstract: These are the Information Assurance Directorate's Top Technology Challenges for 2015.
- Date: 02/24/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/2015-iads-top-tech-challenges.cfm
- Category: IA Guidance > Archive
- SHA256: F7FEB471E97C6F87F92836CA7ABE1351D33381DEA1EE676C9FD8023E3CDBE163
- Size: 266KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for the Graphics Interchange Format (GIF)

- Abstract: This guidance document examines the GIF specifications for data attack, data hiding, and data disclosure risks that exist within the file structure. It provides a breakdown of each component of a GIF file and provides recommendations that can help assure that the GIF file is not only compliant with the specifications but also mitigates these various risks.
- Date: 02/04/2015
- Link: https://apps.nsa.gov/iaarchive/library/reports/gif_isg_v1_0_-20171212.cfm

- Category: Reports
- SHA256: BDDC7B6630A4F089C191740A99C1E08B7A0E19CAB938030A2C5FE7142DA13101
- Size: 997KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Accreditation Portal User's Guide

- Abstract: This guide provides the instructions for using the NSCAP CIRA Accreditation Portal.
- Date: 01/29/2015
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/nscap-accreditaiton-portal-users-guide.cfm
- Category: Supporting Documents
- SHA256: FFBDD1C769210FB89568B36FD1A81307B9082595ECA478399959553824F09C7B
- Size: 4,595KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Defensive Best Practices for Destructive Malware

- Abstract: It is reasonable to expect that organizations, ranging from military to government to industry, will experience an increased threat from destructive malware.
- Date: 01/21/2015
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/defensive-best-practices-for-destructive-malware.cfm

- Category: IA Advisories
- SHA256: 3FD05F21F650D51C2FB735D4FFD17BD8634C64BE34C9E66552CD6342A01EB7DC
- Size: 926KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cyber Incident Response Assistance Accreditation

- Abstract: Program overview briefing slides explaining NSCAP and CIRA; from the 2014 Industry Day.
- Date: 12/10/2014
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/cira-accreditation.cfm
- Category: Supporting Documents
- SHA256: 1C12A3AB8A1BCA3571CAF53C54BC378BFFA00406DCA1A172F11C98EC05276994
- Size: 9,086KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Bash Bug (ShellShock)

- Abstract: A serious vulnerability exists in GNU Bash (Bourne again shell) processes through version 4.3, and CVE-2014-6271 or CVE-2014-7169 exploitation may result in the ability for a remote attacker to override or bypass environment restrictions.
- Date: 10/30/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/bash-bug-shellshock.cfm

- Category: IA Guidance > Security Tips
- SHA256: 34A6E7C947F756792CED6AF2FC92959F163429827CAB97D64670ED922CB70D14
- Size: 337KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Scripting for Bash Vulnerability/Shellshock

- Abstract: Security researchers, vendors, and other reporting organizations have commented on the GNU Bash (Bourne Again shell) vulnerability, the severity of the vulnerability, and the critical need to patch vulnerable versions of Bash. Central to their message is the need to test for the vulnerability by issuing the exploit, and then patching the affected systems. This technical report presents an introduction for technical and non-technical managers who are unfamiliar with the Bash vulnerability. In particular, this note introduces a few sample code fragments that can test for the vulnerability without exploiting the vulnerability.
- Date: 10/28/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/scripting-for-bash-vulnerability-shellshock.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 99C1174E894EBACCC9884038F347398FD91B064C60F7B34201614EC26870F5F4
- Size: 665KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Microsoft’s Enhanced Mitigation Experience Toolkit Guide

- Abstract: Anti-exploitation mitigations like EMET are increasing in importance. By specifically restricting access to broad classes of exploits, EMET protects software from memory corruption attacks used by many APT actors, protects software in between patch cycles, and protects legacy software even without access to the source code.
- Date: 10/22/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/microsoft-enhanced-mitigation-experience-toolkit-a.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 07E804BA9FABCE06FAC0649B64733F5C6F39C6462C4BE03B8E84DA28B430EDAD
- Size: 1,488KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Wireless Vulnerabilities Article

- Abstract: IAD has developed a video entitled “Wireless Vulnerabilities”, MIT-001V-2013. The video addresses the vulnerabilities of using wireless and mobile devices in multiple settings.
- Date: 10/13/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/wireless-vulnerabilities-article.cfm
- Category: IA Guidance > Security Tips
- SHA256: A2030CD0E6495AF1F1D42B78BDE1485BA8AC22A2E1A550A7AE39E9C1C3088F5F
- Size: 28KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Understanding the Enhanced Mitigation Experience Toolkit Frequently Asked Questions

- Abstract: This document contains Frequently Asked Questions regarding EMET
- Date: 10/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/understanding-the-emet-faq.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: A69CFE4F693E572641FF500C97E8C2C8A3DE963CFB2A6CF3F83B9A1B52362B17
- Size: 396KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Microsoft's Enhanced Mitigation Experience Toolkit: A Rationale for Enabling Modern Anti-Exploritation Mitigations in Windows

- Abstract: Microsoft's Enhanced Mitigation Experience Toolkit (EMET) is an enhancement to the Windows operating system that stops broad classes of malware from executing. EMET implements a set of anti-exploitation mitigations that prevent the successful exploitation of memory corruption vulnerabilities in software, including many zero-day and buffer overflow attacks.
- Date: 10/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/microsofts-emet-a-rationale-for-enabling-modern.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: 1D0A10F5C35908D01A16F1A39E8491421043CBEE931D59706C1DC0045CB86C29
- Size: 1,275KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

National Security Cyber Assistance Program Brochure

- Abstract: This brochure provides an overview of the National Security Cyber Assistance Program, CIRA accreditation, and a description of the 21 NSCAP focus areas.
- Date: 09/12/2014
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/brochures/nscap.cfm
- Category: Supporting Documents > Brochures
- SHA256: 689D8CF8FBD61A38723C6DF275C5DFDD19C78FF73372D4667E73100B2A431FC8
- Size: 3,370KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

How National Security Cyber Assistance Program Benefits Service Providers and National Security System Owners

- Abstract: This document lists the benefits of obtaining CIRA accreditation for cyber incident service providers and NSS owners and operators.
- Date: 09/12/2014
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/nscap-cira-accreditation-of-cira-services-providers-benefits.cfm
- Category: Supporting Documents
- SHA256: 0060B3299FDEE423C7353F70484A7877CCE558AD3CEF03FC35BE8AD13A71201E

- Size: 108KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Critical Focus Areas of Cyber Incident Response Assistance

- Abstract: This document provides an overview of the 21 critical focus areas that are part of the NSCAP CIRA accreditation.
- Date: 09/12/2014
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/critical-focus-areas-of-cira.cfm
- Category: Supporting Documents
- SHA256: 092637396E17574D587D102AEC1B5F6E7D9AD1C6398C0D0EC2049C72B9402068
- Size: 846KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cisco Adaptive Security Appliance Out-of-the-Box Security Configuration Guide

- Abstract: This document provides security guidance for network administrator to assist in the initial out-of-the-box configuration of Cisco Adaptive Security Appliance (ASA) 5500 Next Generation Firewalls (software version 9.1). The guidance provided is based on a basic and simplistic security policy for common network architectures; however, the concepts discussed may be applied to complex policies and networks. It is the responsibility of an organization to develop a security policy that meets all of their specific needs. The topics overed are: secure management, interface configuration, auditing and logging, access control and hardening services provided by the Cisco ASA firewall.

- Date: 09/10/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/networks/cisco-asa-out-of-the-box-security-configuration-guide.cfm
- Category: IA Guidance > Security Configuration > Networks
- SHA256: AB0CBCEB4D58CCF5F438399ABA45B527C6682F62F4FD99F3236A7C8847A69487
- Size: 310KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Simple Mail Transfer Protocol (SMTP), Internet Message Format (IMF), and Multipurpose Internet Mail Extensions (MIME)

- Abstract: Provide guidance for the development of an inspection and sanitization software filter for use with email messages. Email servers implement multiple specifications in order to send and receive email, three of which are covered by this document. The Simple Mail Transfer Protocol (SMTP) is used to transmit email from a client to a server. The Internet Message Format (IMF) specifies the format of the email messages, both the headers and the body. The Multipurpose Internet Mail Extensions (MIME) extends IMF beyond plain text. This document introduces the syntax of these standards and then discusses the components that have data hiding, data attack, and data disclosure risks. It provides an analysis of these components and recommendations to mitigate their risks.
- Date: 09/02/2014
- Link: https://apps.nsa.gov/iaarchive/library/reports/email_isg_v1_0-20171212.cfm
- Category: Reports
- SHA256: 51C1C0FAE193122F1A4FF1143DF7B2823B0219AC3B0E15972E00FFE8271A9DB8
- Size: 1,105KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Email Filtering Best Practices Guide Version 1.0

- Abstract: Provide best practices for filtering email messages in boundary protection devices (BPD), including commercial mail gateways, email attachment preprocessors or sidecars, and trusted guard (e.g. cross domain solution (CDS)) components. The guidance in this document is based on over ten years of experience at NSA in developing and testing email BPD's. This experience has provided valuable insight into how email filtering should be implemented in boundary protection devices. This document is a supplement to "Inspection and Sanitization Guidance for Simple Mail Transfer Protocol (SMTP), Internet Message Format (IMF), and Multipurpose Internet Mail Extensions (MIME)."
- Date: 09/02/2014
- Link: https://apps.nsa.gov/iaarchive/library/reports/email_filtering_bpg_v1_0-20171212.cfm
- Category: Reports
- SHA256: 7EA8EFB77B04CD900C3845E6C28A4633179F8544225A4C7F225FC46A7B81EC9C
- Size: 418KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Whitelisting Using Microsoft AppLocker

- Abstract: This guide describes Microsoft AppLocker settings recommended by the NSA's Information Assurance Directorate (IAD) for deploying location-based application whitelisting on your network. Alternative application whitelisting implementations that may support your organizational needs are commercially available. These alternative implementations may provide support to multiple different operating system platforms for a fee. This guide also provides administrators with a walkthrough on how to use AppLocker

and implement the settings. Using AppLocker for application whitelisting enforcement will not stop all malicious software. It provides an additional layer in a defense-in-depth strategy. The intent of this guidance is to prevent users from unknowingly or accidentally executing malicious code or unauthorized software.

- Date: 08/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 05D8F19F3A55E4F2C5BD27C8F1B262FC608ECE4F6FA5E63E04748EA344119072
- Size: 1,748KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network

- Abstract: United States Critical Infrastructure faces a significant risk from the exploitation of Structured Query Language (SQL) injection vulnerabilities. If executed successfully, an SQL injection may allow for the compromise of confidentiality, integrity, and availability of a database and its contents; an outcome that may carry a high cost in system recovery and reconstitution, data restoration, downtime, regulatory penalties, and negative publicity. Due to the manageable level of complexity of SQL injection, the array of freely available tools that automate the exploitation process, and the techniques' demonstrated potential for impact, malicious cyber actors will continue relying on SQL injection vulnerabilities in public facing websites as a means of gaining access to critical infrastructure systems and networks.
- Date: 07/23/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/defending-against-the-exploitation-of-sql-vulnerabilities-to.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 398F0F97A7FBCA22C5C22B613ED3AF7AD66361C6B036D8FFC7A4CC7DA317471C

- Size: 2,988KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

2014 IAD's Top Technology Challenges

- Abstract: This document is a list of IAD's top technology challenges in 2014.
- Date: 07/06/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/2014-iad-top-technology-challenges.cfm
- Category: IA Guidance > Archive
- SHA256: 3ED796CDED01B5F57C788A1CADE0F8CE85BD35BF179E702FDDC774F3917A4C09
- Size: 173KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Information Assurance Guidance for Microsoft Windows XP End of Life

- Abstract: This document provides instructions for what to do with Windows XP machines at the end of their life.
- Date: 07/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/ia-guidance-for-microsoft-windows-xp-end-of-life.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 385B6A9FE64AD46643836872AD283883383DA660742A8B834E0B4CE920EFBA5D
- Size: 417KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Community Gold Standard 2.0

- Abstract: CGS provides comprehensive IA guidance for securing NSS enterprises and enables the mission in the face of continuous attack. CGS characterizes the best practice for IA capabilities in accordance with policies and standards, while considering the limitations set forth by current technologies and other constraints.
- Date: 06/26/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-standards/cgs/community-gold-standard-framework.cfm
- Category: IA Guidance > IA Standards > Community Gold Standard
- SHA256: 689EE4DE6E7C1DDA980D249DBE20D28E29A7161F1C94515A47779A87CFF8A43B
- Size: 1,558KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Identity Theft Threat and Mitigations

- Abstract: This document contains information about the threat of identity theft and how to prevent it.
- Date: 05/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/identity-theft-threat-and-mitigations.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: E66DC20BD55760CAE33EB3856ED0209AEAF1F769D246EDB3F19CE2D8CDA1FDBD

- Size: 2,374KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Factsheet: Mitigations for OpenSSL TLS/DTLS Heartbeat Extension Vulnerability

- Abstract: This update provides further clarification of the Mitigations for OpenSSL TLS/DTLS Heartbeat Extension Vulnerability Update.
- Date: 05/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/mitigations-for-openssl-tls-dtls-heartbeat-extension.cfm
- Category: IA Guidance > Security Tips
- SHA256: FA9F4089D22A1FBD4FA3E5F36DECF90A8AE149CC2470AAD8A9A7C7E215E459E1
- Size: 236KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Best Practices for Keeping Your Home Network Secure

- Abstract: This document contains information about best practices in order to keep your home network secure.
- Date: 05/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/best-practices-for-keeping-your-home-network-secure.cfm
- Category: IA Guidance > Security Tips
- SHA256: E97985B6AE094245ECD2BCA90D28F89CB1D708E7622DB9EEE5FAFC585C3C768D

- Size: 1,894KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Journal of Information Warfare, Vol. 13 Issue 2

- Abstract: To all readers, we are very excited about this issue. This is a special edition of the Journal of Information Warfare (JIW) and the first of its kind where we have collaborated with the Information Assurance Directorate (IAD) of the National Security Agency (NSA). In this publication, we bring you 10 articles from current and highly technical subject matter experts from NSA, all of which focus on cyber-security efforts that attempt to realize their theme of Confidence in Cyberspace. We hope you enjoy this special issue, and it is our desire to continue this new effort as an annual tradition.
- Date: 04/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/journal-of-information-warfare.cfm
- Category: Supporting Documents
- SHA256: B41E3353C60FB848E712F11E9E2B83052C2868CE9B3C6CEB7AC85F5EA2C790CC
- Size: 3,484KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Supplemental Guide to the National Manager's Letter 2014

- Abstract: This supplement provides guidance in priority order based on effectiveness in countering/containing adversary impact.
- Date: 03/21/2014

- Link: https://apps.nsa.gov/iaarchive/library/reports/supplemental-guide-to-the-national-managers-letter.cfm
- Category: Reports
- SHA256: 7DC7B46D45DA3CC4458541E4F5299F72CF8A249D4CF5DE8F897E9EE8846F2875
- Size: 773KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Supplemental Guide to the National Manager's Letter 2015

- Abstract: National Security Directive 42 (NSD-42) and Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Infomation) mandates the National Manager develop effective technical safeguarding policies and standards that address the safeguarding of information within NSS and assess the overall security posture of NSS.
- Date: 03/20/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-standards/cgs/supplemental-guide-to-the-national-managers-letter-15.cfm
- Category: IA Guidance > IA Standards > Community Gold Standard
- SHA256: 4030A6A6265A08AFD1280512D2F2A2BD848DEA8354B3B36D3269555E7C60F2D4
- Size: 1,862KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Random Number Generators: Introduction for Operating System Developers

- Abstract: Key material generation is as important to strong cryptosystems as the algorithms used. Weak random number generators (RNGs) have been known to create key material that is guessable by adversaries1, making the strength of the algorithms irrelevant in cryptographic attacks. This paper, intended for operating system developers, provides an overview of considerations developers should be making when designing and using RNGs, outlines how RNGs work, and gives recommendations for developing and using RNGs.
- Date: 03/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/random-number-generators-introduction-for-operating-system.cfm
- Category: IA Guidance > Security Tips
- SHA256: A0CAFA06635E42C20F984502DD038B8DCD1088ED5499698D34A33F9F5058C153
- Size: 644KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Random Number Generators: Introduction for Application Developers

- Abstract: Key material generation is as important to strong cryptosystems as the algorithms used. Weak random number generators (RNGs) have been known to create key material that is guessable by adversaries1, making the strength of the algorithms irrelevant in cryptographic attacks. This paper, intended for application developers, provides an overview of considerations developers should be making when using RNGs, outlines how RNGs work, and gives guidance for applications needing RNG services.
- Date: 03/01/2014
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/random-number-generators-introduction-for-application.cfm
- Category: IA Guidance > Security Tips
- SHA256: 8E94365FB3B9B62D3FC4518694C7DF14D1C9F750A62B0BCFB2519DD9DD511324
- Size: 582KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for the Wavelet Scalar Quantization (WSQ) Biometric Image Format

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for Wavelet Scalar Quantization (WSQ) biometric files. WSQ is a compression algorithm formally defined in the Criminal Justice Information Services (CJIS), WSQ GRAY-SCALE Fingerprint Image Compression Specification, IAFIS-IC-0110(V3). This document also refers to WSQ as a file type, since the data representing the entire image defined in is also commonly stored within a file. This document analyzes various elements and objects that are contained within the WSQ file structure and then discusses the data hiding, data attack, and data disclosure risks. It describes how those elements can be a cause for concern for either hiding sensitive data or possibly attempting to exploit a system.
- Date: 01/22/2014
- Link: https://apps.nsa.gov/iaarchive/library/reports/wsq_isg_v1_0_20171212.cfm
- Category: Reports
- SHA256: 3955D27DD4680DEDF4F0E69BDF3489AA4DAA55213B33393F8CA7162A3D94B749
- Size: 610KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Spotting the Adversary with Windows Event Log Monitoring

- Abstract: This paper focuses on using the built-in tools already available in the Microsoft Windows operating system (OS). Central event log collection requires a Windows Server operating system version 2003 R2 or above. Many commercially available tools exist for central event log collection. Using a Windows Server 2008 R2 or above server version is recommended. There are no additional licensing costs for using the event log collection feature. The cost of using this feature is based on the amount of additional storage hardware needed to support the amount of log data collected. This factor is dependent on the number of workstations within the local log collection network.
- Date: 12/16/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/spotting-the-adversary-with-windows-event-log-monitoring.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: E7FF70328E660A05F0BE079DB72AEBA04AF5769E4856FFD34FBD1EFF77EFA95B
- Size: 871KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Host Mitigation Package

- Abstract: Host Mitigations Package (HMP) is designed to aid organizations and system administrators in hardening their host systems.
- Date: 12/01/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/host-mitigation-package.cfm
- Category: IA Guidance > Security Tips
- SHA256: BA098FD3774DD98FC45E4948213F32580DEA0C751885002AC7541CB8AD41B499
- Size: 1,288KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Reducing the Effectiveness of Pass-the-Hash

- Abstract: This document discusses mitigations administrators can deploy, in the interim, to reduce PtH's effectiveness by addressing some of the properties it depends upon.
- Date: 11/19/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/reducing-the-effectiveness-of-pass-the-hash.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: 2BB4F682A2C48485E332FC0A2FA9E4DDD00B8520424670EF9F588986779ED51A
- Size: 350KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Web Domain Name System Reputation

- Abstract: Danger could be lurking behind any website. Cyber adversaries routinely hack into legitimate websites or create their own malicious sites to upload malware to the computers of unsuspecting web visitors.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/web-domain-name-system-reputation.cfm
- Category: IA Guidance > Security Tips

- SHA256: BF05F3E2928AD32B80A91A6C6733D4200761037C2FCE8F3BE89B631E877F0B91
- Size: 712KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Segregate Networks and Functions

- Abstract: After gaining initial access to a network, adversaries traverse the allowed communication paths between network devices to gain deeper access. However, a securely segregated network can greatly reduce an adversary's ability to access sensitive portions of the network.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/segregate-networks-and-functions.cfm
- Category: IA Guidance > Security Tips
- SHA256: F9CA6B526232EDD75189374954AB8A8405F541C54968E5F6920EA05AF200110D
- Size: 414KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Secure Host Baseline

- Abstract: A Secure Host Baseline (SHB) is a pre-configured and security hardened machine-ready image that contains an organization's common Operating Systems (OS) and application software.
- Date: 10/31/2013

- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/secure-host-baseline.cfm
- Category: IA Guidance > Security Tips
- SHA256: AE1ABE6B565A06481068200591DFF4F2A55FB2EAED6ED82061D635B33A291CEB
- Size: 491KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Limit Workstation-to-Workstation Communication

- Abstract: Compromise of just one user workstation can lead to the loss of an entire network. All it takes is an unsuspecting user to click on a malicious email attachment or visit an infected website for an adversary to obtain access to a single workstation.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/limit-workstation-to-workstation-communication.cfm
- Category: IA Guidance > Security Tips
- SHA256: F00FE75B80B9F9FF5486E3D0AA46B4D0DF252C23995E6F1191E1A6DFE2E5C1CA
- Size: 502KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Host Intrusion Prevention Systems

- Abstract: maintaining the health or integrity of individual hosts — HIPS is a valuable component used to defend computer host integrity.

- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/host-intrusion-prevention-systems.cfm
- Category: IA Guidance > Security Tips
- SHA256: 68CF00497DF4848315D922250808D0998600DE80BE6309583947492F04D7EED8
- Size: 618KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Control Administrative Privileges

- Abstract: Administrative privileges on a computer system allow access to resources that are unavailable to most users and permit the execution of actions that would otherwise be restricted.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/control-administrative-privileges.cfm
- Category: IA Guidance > Security Tips
- SHA256: 545BACA6224B06902BA3B6DB75AF1A815B27026EFC3BA769CE3903F6A79E7FEE
- Size: 655KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cloud Security Considerations

- Abstract: Cloud services are a recent model for information technology implementation and management. The cost advantages are a driving force, with security often as a secondary consideration.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/cloud-security-considerations.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: ACCE0635A0A94CD69029FC78F53DD368C2C16847880335346AF14D62490AFE0F
- Size: 1,046KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Whitelisting

- Abstract: Application Whitelisting is a proactive security technique that only allows a limited set of approved programs to run, while blocking all other programs (including most malware) from running by default.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/application-whitelisting.cfm
- Category: IA Guidance > Security Tips
- SHA256: 786ABDB394F7FD5466467E43C4BCF689C78C806E6258E283D884867396E68F40
- Size: 597KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Anti-Virus File Reputation Services

- Abstract: In today's netspeed environment, traditional antivirus protection is not enough. The majority of antivirus products rely on signature or hash-based methods of detecting "known-bad" activity or files.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/anti-virus-reputation-services.cfm
- Category: IA Guidance > Security Tips
- SHA256: 8BF78496DB0B04D46C552AE41D44A9F2C3248989D36BDA060F719B4D6CF017B5
- Size: 528KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Anti-Exploitation Features

- Abstract: Cyber attackers want access to your sensitive information or intellectual property for strategic advantage, or more commonly, for monetary gain. They commonly attempt to exploit vulnerabilities in your computer system and network by using malware delivered via email or web servers.
- Date: 10/31/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/anti-exploitation-features.cfm
- Category: IA Guidance > Security Tips
- SHA256: CBECB51432EF1C4C9EB1447CD043B0D09ACDDEB8E1546BEE0066629FAFC57532
- Size: 520KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Recommendations for Configuring Adobe Acrobat Reader XI in a Windows Environment

- Abstract: This document includes information for using Adobe's Customization Wizard (CW) or Microsoft's PowerShell to configure the necessary settings for uniform distribution of the software throughout an enterprise or on a standalone system. Appendix A lists all of the ARXI security-related settings with recommendations for the environments that should configure those settings.
- Date: 07/12/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/recommendations-for-configuring-adobe-acrobat-reader-xi-in-a.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: EE255022F471D504707C704E7E4B93C5CA72AD5D54F49F5352F650BCA163B3DC
- Size: 330KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Building Web Applications Security Recommendations for Developers

- Abstract: This document provides recommendations for web developers on how to build and deploy secure web applications in order to counter this threat.
- Date: 04/15/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/building-web-applications-security-recommendations-for.cfm
- Category: IA Guidance > Security Tips
- SHA256: 77E02E84DEF7739C4AB4FAE874F7CA88C9B530A375B0EE60D6CC72C052BF4D67
- Size: 534KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Host Based Security System Application Whitelisting Technical Implementation Guide

- Abstract: This guide is intended to be used as a reference in implementing location-based application whitelisting using HBSS HIPS.
- Date: 03/01/2013
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/hbss-application-whitelisting-technical-implementation-guide.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 67AEF858E461A9EDA56811493CF71A2960C94A08DB4F3785FBFA177F594B7D91
- Size: 7,020KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for HyperText Transport Protocol (HTTP)

- Abstract: The purpose of this document is to provide guidance for the development of an inspection and sanitization software tool for the HyperText Transport Protocol (HTTP). It introduces the syntax of the protocol and then discusses the components that have data hiding, data attack, and data disclosure risks. This document provides an analysis of these components and recommendations to mitigate their risks.
- Date: 11/27/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/http_inspection_and_sanitization_guidance_v1_1-20171212.cfm
- Category: Reports

- SHA256: 9B0CB994A63A3195C944713721472F30CD22B5436E834D4BE3991127A1BA610C
- Size: 1,004KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for JPEG 2000

- Abstract: This document outlines the findings of potential areas of concern that exist within the JPEG 2000 file format. It also provides inspection and sanitization guidance for JPEG 2000 image files to address data attack, hiding, and disclosure risks. This document does not address any potential security risks of the JPEG 2000 compression/encoding algorithm, but focuses more on the actual format as a container for the compressed/encoded image data.
- Date: 11/27/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/jpeg_2000_inspection_and_sanitization_guidance_v1_4_4-20171206.cfm
- Category: Reports
- SHA256: E6ECA43D0CD60FE0AF1E8C5D3152C85DB36BCB048DF807B7EA69B907D75E2D43
- Size: 743KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Deploying Signed BIOSes to Enterprise Client Systems

- Abstract: This guide is meant to assist United States government and Department of Defense Windows system administrators deploy BIOSes to their enterprise client systems that support signed BIOSes and signed BIOS update mechanisms but do not have signed

BIOSes installed by default due to these systems predating the NIST SP 800-147 standard. Vendors that implement signed BIOses currently ship systems with a signed BIOS already installed. This guide also provides information on tools for managing BIOSes that are freely available and officially supported by vendors for commercial use. The guide assumes administrators operate in a restrictive network environment where common remote management protocols may be blocked and common automation technologies may be disabled. Very basic techniques and technologies are used in this guide to apply to the widest audience possible and to allow easier integration into restrictive environments.

- Date: 11/16/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/deploying-signed-bioses-to-enterprise-client-systems.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: 4E9D20F3F7167ADD4BB92AB8510B6F6B536F4865FEF66012AB7E3AAEF2111D3A
- Size: 359KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for JPEG File Interchange Format

- Abstract: This document is meant to provide guidance for the development of software tools to analyze and mitigate potential security risks in the JPEG File Interchange Format (JFIF) version 1.02. These guidelines come from the evaluation of the format specification, not from any vendor specific implementation or software application.
- Date: 11/07/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/jfif_jpeg_inspection_and_sanitization_guidance_v1_0-20171206.cfm
- Category: Reports
- SHA256: 20CAFDB9909EEF5CF188004BF838B837DFAC006FA019C01A68A4DBF9AD2DEE50

- Size: 639KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

JavaScript Security Risks

- Abstract: This document addresses the issues that JavaScript introduces into a document format. It shows how basic JavaScript can be manipulated and obfuscated to evade signature detection, by using publically available and known methods. Code that introduces both a data hiding and data attack risk can be difficult to detect, especially when the code is obfuscated. This paper presents some known methods to mitigate the risk of running JavaScript; however, at the moment, more research is needed to develop a more robust solution.
- Date: 11/07/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/javascript_security_risks_v1_1-20171212.cfm
- Category: Reports
- SHA256: B633B5EF2BD465EBC00B599A51AC4D4167D438CB2CEDD59B1E90F7FEC9768269
- Size: 1,021KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Configuring Windows To Go as a Mobile Desktop Solution

- Abstract: Windows To Go is a new feature of Windows 8 Enterprise that allows a fully functional Windows 8 instance to be run from an external USB flash drive. When a host machine is booted from a Windows To Go drive, the user experience is the same as the

Windows 8 Enterprise desktop. This document provides uses cases, security and administrative considerations, configuration recommendations, and instructions for creating a secure Windows To Go device.

- Date: 11/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/configuring-windows-to-go-as-a-mobile-desktop-solution.cfm
- Category: IA Guidance > Security Tips
- SHA256: 468B4D87EB1290633139BDE1C116C5BA8B84EAD746DECF0B89CA75F800780CD4
- Size: 420KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Deploying and Securing Google Chrome in a Windows Enterprise

- Abstract: This paper contains deployment guidance, recommended policies, and technical details for United States government and Department of Defense administrators who want to use the enterprise version of the Google Chrome web browser in their Windows Active Directory domain. Chrome 20.0.1132.47,
- Date: 10/22/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/deploying-and-securing-google-chrome-in-a-windows-enterprise.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: FF8CB00DE6AADB4B27CD37ADF0A4A5168593AE28DA739F6B98B1B2C5C1542156
- Size: 725KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Community Gold Standard Brochure

- Abstract: Community Gold Standard Brochure
- Date: 10/16/2012
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/brochures/community-gold-standard-for-information-assurance.cfm
- Category: Supporting Documents > Brochures
- SHA256: 3D4E5A66A53B01BDAF550CC22AB96929CFB39BFFE750C88EC96585561647192D
- Size: 4,396KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Securing Data and Handling Spillage Events

- Abstract: Data spillage is the transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications, or media. A spillage can be from a higher level classification to a lower one. The data itself may be residual (hidden) data or metadata. Spillage may result from improper handling of compartments, releasability controls, privacy data, or proprietary information.The trend towards increased information sharing has weakened access controls, giving users without a need-to-know access to large volumes of sensitive or classified data. Malware that propagates via removable media has increased the risk of large data transfers outside the network. The risk of data spillage is a problem largely because of inadequate end user security awareness, unmanageable networks, and poorly implemented data policies.
- Date: 10/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/securing-data-and-handling-spillage-events.cfm
- Category: IA Guidance > Security Tips

- SHA256: BFD74146BB200A942CB0953BC073B85F41926E159C8B3006BA29A33B540C3C65
- Size: 673KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Hardening Authentication

- Abstract: This document contains information on how to harden authentication processes by limiting remote access, augmenting authentication measures, educating users, hardening the authentication servers, and establishing robust authentication policy.
- Date: 09/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/hardening-authentication.cfm
- Category: IA Guidance > Security Tips
- SHA256: 1E7734A6F6EFCB7330010301E746CB1E5C8E05D1C2F847591CC44D254A393771
- Size: 708KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mobile Device Management: Capability Gaps for High-Security Use Cases

- Abstract: This paper, intended for mobile device platform vendors as well as risk decision makers, provides an overview of MDM platform components and then outlines these gaps in capability.
- Date: 08/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/mobile-device-management-capability-gaps-for-high-security.cfm

- Category: IA Guidance > Technical Briefs
- SHA256: 9C4A32E716C0FF15CCAA9D6B8F0668D5A480975EFE2DE0E45FA011DDC2DDA9EA
- Size: 734KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mobile Device Management: A Risk Discussion for IT Decision Makers

- Abstract: This document describes the high-level architecture and capabilities of MDM solutions, and introduces key security issues to consider when deploying them.
- Date: 08/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/mobile-device-management-a-risk-discussion-for-it-decision.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 77C15151C4883363DAC6540440074D6445B35A4684B59C20DC789ED54E5770A3
- Size: 734KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Defending Against Compromised Certificates

- Abstract: This guidance provides IT personnel with actionable information to defend against compromised CA and web site certificates, which could permit a malicious web server to impersonate the genuine one. Each operating system (OS) and browser may use different mechanisms to check and revoke trust in a certificate. Some use a Certificate Revocation List (CRL), while others

use the Online Certificate Status Protocol (OCSP). Still others rely entirely on the issuance of software updates, whose prompt application remains fundamentally important. Variety also exists in how browsers handle certificate validation. Some query the OS certificate store, while others use their own certificate store and thus must be configured separately. Finally, note that some sites may become inaccessible when enforcing strict revocation checking.

- Date: 07/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/defending-against-compromised-certificates.cfm
- Category: IA Guidance > Security Tips
- SHA256: 35352C620F1BF03BA3E32FA3AAF1F12069387110890510579 40F9BF8BDBCE0A1
- Size: 306KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Guidelines for Regular Expressions in XML Schemas

- Abstract: This report informs developers about security issues with regular expressions. Armed with this knowledge, developers will be able to create safe regular expressions. This report also informs accreditors (particularly those who assess XML Schemas for compliance with security policies) about the kinds of security issues involved with regular expressions in XML Schemas.
- Date: 06/30/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/guidelines_for_regular_expressions_with_xml_schemas_v1_0.cfm
- Category: Reports
- SHA256: EC32D7FC3286B5DBEDD0FB73AF6BBD31A0911A2207586DF6EBA1EB9F35AEC2CE
- Size: 964KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

XSLT 1.0 Recommendations for Making XSLT Programs Behave as Expected

- Abstract: This paper provides recommendations for writing XSLT programs that will behave in an expected manner. However, it is not a general tutorial on how to write an XSLT program. The paper also identifies some known XML-related risks or concerns that can be mitigated with XSLT programs. In addition to a set of recommendations, the paper contains a “how to” section that shows how to use XSLT to perform common risk reduction tasks. These recommendations and samples of XSLT source code apply only to XSLT version 1.0.
- Date: 06/29/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/xslt-guidance_v1_0-20171212.cfm
- Category: Reports
- SHA256: F3BE3AE4F60C32912B8A9BE4BCA6C71827EED4210155335D0641BB3B94686543
- Size: 684KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Using Schematron for Cross Domain Security Policy Enforcement

- Abstract: This document provides recommendations for using Schematron schemas to enforce data constraints on the contents of Extensible Markup Language (XML) documents being transferred between security domains. Schematron is a rule-based schema language used for making assertions about patterns found in XML documents. The risk of transferring invalid or unauthorized XML data into or out of a sensitive security domain can be reduced by validating the XML data against a schema that fully describes and constrains the data. These more restrictive schemas are not necessarily the same as those that might be used to validate data being transferred within a single security domain. Schematron can be used as part of a Cross Domain Solution (CDS) to address security problems that may be difficult to solve using grammar-based XML Schema languages.

- Date: 06/29/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/schematron_cross_domain_policy_enforcement_v1_0-20171212.cfm
- Category: Reports
- SHA256: 8E0A585DE1B15A62FAA89E99654D46C2E273F2DB87EEE09AAF9FAD299ADD43AA
- Size: 623KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Basic XML Security Considerations

- Abstract: This document presents fundamental information about XML and discusses how these fundamental truths influence XML security. The document then describes a range of XML security issues, including several that are sometimes overlooked. By referring to this document, a reader can become better informed about which security concepts apply to a given use case and obtain recommendations for implementing those security concepts. Perhaps more importantly, the reader will become aware of what XML does not inherently provide.
- Date: 06/28/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/basic-xml-security-considerations_v1_0_20171212.cfm
- Category: Reports
- SHA256: 753B5C34F6F42F548C13AFBD4BDB10F8C26B9402F4617C2B2AD0C353259BEF74
- Size: 278KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Frank B. Rowlett Award for Individual Excellence Nomination Form

- Abstract: Nomination procedures for Rowlett Awards - Individual instruction booklet
- Date: 05/04/2012
- Link: https://apps.nsa.gov/iaarchive/library/supporting-documents/forms-templates/frank-b-rowlett-award-for-individual-excellence-nomination.cfm
- Category: Supporting Documents > Forms Templates
- SHA256: FE524339F2594136CCD3BB81E289B8A9CC996A9FBBB92E2B743A94952C06BFA5
- Size: 2,425KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Content Automation Protocol Content for Apple iOS 5 Security Configuration Recommendations

- Abstract: These are zip files that go with the Apple iOS configuration guide
- Date: 05/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/associated-scap-content-for-apple-ios-5.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: E662913C4450085E0F2C0164DB7C561B7B711C33B177ECFA812B795B899860CF
- Size: 29KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

New Smartphones and the Risk Picture

- Abstract: Mobile phone platforms are susceptible to malicious attacks, both from the network and upon physical compromise. Understanding the vectors of such attacks, level of expertise required to carry them out, available mitigations, and impact of compromise provides a background for certain risk decisions. In general, comparing risks introduced by the new generation of mobile devices to those of traditional, widely-deployed desktop systems provides insight into how the risks to DoD networks are changing. Due to the larger cultural and technological shift to mobile devices, this may be more relevant than comparison of diff erent smartphone brands.
- Date: 04/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/new-smartphones-and-the-risk-picture.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: B10DEDE4D95744C8D67EA818955C13AA3EE746CAB53647F921E30404288454F8
- Size: 982KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Configuration Recommendations for Apple iOS 5 Devices

- Abstract: This document provides security-related usage and configuration recommendations for Apple iOS devices such as the iPhone, iPad, and iPod touch.
- Date: 03/28/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/security-configuration-recommendations-for-apple-ios-5.cfm

- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: A5594890D800D797602108827AF9D367E4FFF049DB859B3D4544A2E130B6C9FB
- Size: 235KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for HyperText Markup Language (HTML)

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for HyperText Markup Language. It introduces the syntax of various elements within the language and then discusses several elements that have data hiding, data attack, and data disclosure risks. This document provides an analysis of these elements and recommendations to mitigate their risks.
- Date: 03/02/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/html_inspection_and_sanitization_guidance_v1_0-20171212.cfm
- Category: Reports
- SHA256: FEE653A1BA7669684C4A96D8B1880D1390ABB6B368B614039D32400DEFD921C7
- Size: 1,559KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Cascading Style Sheets

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for Cascading Style Sheets (CSS), which may exist within or external to HyperText Markup Language (HTML) documents.
- Date: 03/02/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/css2_inspection_and_sanitization_guidance_v1_0-20171212.cfm
- Category: Reports
- SHA256: B1278D84FBF2736BF3062308BF254F0A578B02ADC1E7C891128DF9601EF4932F
- Size: 937KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Bitmap File Format

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for the Bitmap (BMP) images as defined in the Microsoft Developer Network Bitmap Reference. It provides inspection and analysis on various elements that are contained within the BMP file structure and how they can be a cause for concern for either hiding sensitive data or attempts to exploit a system. This document provides an analysis of features in BMP and recommendations to mitigate these threats to provide a safer file. Although this report does not mention vulnerabilities related to a specific image editor, many were used in the analysis of the BMP file format. Numerous Common Vulnerabilities and Exposures (CVE)s have registered for BMP related vulnerabilities in applications.
- Date: 03/02/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/bmp_inspection_and_sanitization_guidance_v1_0-20171212.cfm
- Category: Reports
- SHA256: 9B84C729F13A4F016E3CFA03905E8A4147D2A462F3C2314D378935260CCC36B2
- Size: 654KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Waveform Audio File Format

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for the WAVE file format. It provides inspection and analysis guidance on the various constituents that are contained within the WAVE file structure and describes how they can be a cause for concern for either hiding sensitive data or attempts to exploit a system.
- Date: 03/02/2012
- Link: https://apps.nsa.gov/iaarchive/library/reports/wave_inspection_and_sanitization_guidance_v1_0-20171206.cfm
- Category: Reports
- SHA256: 78EC7E3E1DCA47A1B142C2BF85D681C00978623D7DA92A3731BE288C9545AF9C
- Size: 1,397KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Rich Text Format (RTF)

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for the Rich Text Format (RTF). It provides analysis of the various elements and objects that are contained within the RTF file structure and how they can be a cause of concern for data attack, data hiding, and data disclosure. This document provides recommendations to mitigate these risks. Although this report does not cover vulnerabilities related to a specific RTF capable software application, a number of them were used in the analysis of the standard.
- Date: 03/02/2012

- Link: https://apps.nsa.gov/iaarchive/library/reports/rtf_inspection_and_sanitization_guidance_v1_0.cfm
- Category: Reports
- SHA256: F2E4DB9392CD878CB9F5669F6D055312411CAC1E1B40699E26EDDCBB9D0E053B
- Size: 1,068KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mitigation Monday #3: Defense against Malware on Removable Media

- Abstract: This mitigation report presents a common attack scenario for Microsoft Windows networks, the use of malicious removable media by an adversary. It also discusses how it can be prevented using a defense-in-depth strategy.
- Date: 03/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/defense-against-malware-on-removable-media.cfm
- Category: IA Guidance > Security Tips
- SHA256: B206F3D0294AF94C2957FC4D98C3BCC826633233D67DFC8E2AD70E12F0F4A94B
- Size: 692KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Tips for Personally Managed Apple iPhones and iPads

- Abstract: This pamphlet provides security recommendations for users of personally managed Apple iPhones and iPads running iOS 5. This refers to a situation in which the user exercises sole administrative control over the device.

- Date: 01/01/2012
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/security-tips-for-personally-managed-apple-iphones-and-ipads.cfm
- Category: IA Guidance > Security Tips
- SHA256: 5E6A22DFBC433A769C62E3D144809E27C376B884B39BDC77D32E9542D84D4456
- Size: 255KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Redaction of Portable Document Format Files Using Adobe Acrobat Professional X

- Abstract: This document describes a procedure using Adobe Acrobat Professional X to redact information from PDF documents. The original source of the document can be any application, but the process described applies to documents that are already in PDF.
- Date: 11/22/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/redaction-of-pdf-files-using-adobe-acrobat-professional-x.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: E6916EF1D29B28A1C9028D42933F1948AA6D92D9BF173260AF497BC0C74BB654
- Size: 809KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Hardening Deployed Web Applications

- Abstract: With the ever increasing attacks on Commercial Networks targeting web applications, it is important to verify that the appropriate actions are being implemented to harden a web server from these types of intrusions.
- Date: 09/12/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/hardening-deployed-web-applications-report.cfm
- Category: IA Advisories
- SHA256: 8C4F9AA8D02702276363AE09973C299F87B3222818C2DAE7E53C030284533FBF
- Size: 6,311KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Protect Against Cross Site Scripting Attacks

- Abstract: Cross Site Scripting (XSS) is a vulnerability in web applications that allows an attacker to inject HTML, typically including JavaScript code, into a web page. XSS results from the intermingling of server code and user input. If user input is not sanitized correctly, it could contain code that runs along with server code in a client's browser. In 2010, XSS was ranked the #2 web application security risk by the Open Web Application Security Project (OWASP) and the #1 software error by the SANS Institute. This factsheet explains ways to mitigate XXS attacks.
- Date: 09/01/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/protecting-against-xss-attacks.cfm
- Category: IA Guidance > Security Tips
- SHA256: FEC35BFD0AA0589B76C61C21A332B0DCF98FBCDCB721A1F98F272DEE24692A08
- Size: 349KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Guide to the Secure Configuration of Red Hat Enterprise Linux 5

- Abstract: The purpose of this guide is to provide security configuration recommendations for the Red Hat Enterprise Linux (RHEL) 5 operating system. The guidance provided here should be applicable to all variants (Desktop, Server, Advanced Platform) of the product. Recommended settings for the basic operating system are provided, as well as for many commonly-used services that the system can host in a network environment. The guide is intended for system administrators. Readers are assumed to possess basic system administration skills for Unix-like systems, as well as some familiarity with Red Hat's documentation and administration conventions. Some instructions within this guide are complex. All directions should be followed completely and with understanding of their effects in order to avoid serious adverse effects on the system and its security.
- Date: 08/26/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/guide-to-the-secure-configuration-of-red-hat-enterprise.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: AD051932BFED72FC72D58F3E502C869568B54A1AD3B14FD257788932D402ED9F
- Size: 867KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Enforcing No Internet or E-mail from Privileged Accounts

- Abstract: Browsing the Internet or reading e-mail with admin, root, or other elevated privileges is a very serious security risk! Malicious websites, e-mails, and e-mail attachments can quickly make use of the elevated privileges to install malware throughout the network.
- Date: 08/01/2011

- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/enforcing-no-internet-or-e-mail-from-privileged-accounts.cfm
- Category: IA Guidance > Security Tips
- SHA256: 9E064286303BA94974AB25BB88857AA03F268A5C97C2DD8B4A9910E115E4D1F9
- Size: 539KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Host Protection Technology Study

- Abstract: This study examined the behavior and capabilities of the different technologies against various attack scenarios in order to determine their effectiveness. The various products were grouped into different technology categories (host firewall, virus scanner, etc) and installed in a controlled environment. A sample set of attack scenarios was constructed and tested against the various technologies. Because of the pervasive use of Microsoft windows on desktop hosts, this study focused on Windows attacks and protection tools. Results were recorded and analyzed and a summary is presented in this document.
- Date: 06/01/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/host-protection-technology-study.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 47BAA8F3F6F18DE5C90E21B8F7B55E6A9DDE09696D91A3F84048A6E3667E3044
- Size: 3,398KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Security Guidance for the use of XML Schema 1.0/1.1 and RELAX NG

- Abstract: This document provides guidance for creating Extensible Markup Language (XML) Schemas and Regular Language for XML Next Generation (RELAX NG) schemas that can be used to describe the format and contents of XML documents being transferred between security domains. The risk of transferring invalid or unauthorized XML data into or out of a sensitive security domain can be reduced by validating the XML data against a schema that fully describes and constrains the data. These more restrictive schemas are not necessarily the same as those that might be used to validate data being transferred within a security domain. As the popularity and usage of XML grows, so too will Cross Domain Solutions (CDS) that filter via schemas also grow; however, using poorly written schemas can undermine the security functionality of even the most well designed CDS.
- Date: 05/11/2011
- Link: https://apps.nsa.gov/iaarchive/library/reports/xml_schema_1-1_relax_ng_security_guidance_v1_0_1-20171212.cfm
- Category: Reports
- SHA256: 8E75584AB372AC93C531E6B39EC2A57E94D41459676AC4FCE02E3664B8838CD0
- Size: 1,146KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Portable Document Format

- Abstract: The purpose of this document is to provide guidance for the development of a sanitization and analysis software tool for the Portable Document Format (PDF). It provides inspection and analysis on various elements and objects that are contained within the PDF file structure and how they can be a cause for concern for either hiding sensitive data or attempts to exploit a system. This document provides an analysis of numerous features in PDF and also provides recommendations to mitigate these threats to provide a safer file. Although this report does not mention vulnerabilities related to a specific PDF reader software application, however there were a number of them used in the analysis of the standard.
- Date: 05/02/2011
- Link: https://apps.nsa.gov/iaarchive/library/reports/pdf_inspection_and_sanitization_guidance_v1_0-20171206.cfm

- Category: Reports
- SHA256: 9240BD0B2F698DBDEB168630045203D05C72108C1DCD5E615650108A6E043A0B
- Size: 2,141KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Guidelines for Implementation of REST

- Abstract: This paper tries to help identify and explain the security risks (positive and negative) with REST, to facilitate development of more robust REST solutions.
- Date: 03/25/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/guidelines-for-implementation-of-rest.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: 1ADC85C039894D2F0960200954D4AF9264717145C3528D72823AE8D47D5BB770
- Size: 708KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

BIND 9 Domain Name System Security

- Abstract: Vulnerability Technical Reports such as BIND 9 Security provide our customers with value-added information regarding a plethora of technologies. These reports identify vulnerabilities and provide recommendations to improve or eliminate the identified vulnerabilities. These reports also prioritize vulnerabilities and identify future initiatives in that particular technology arena. BIND is an

open-source Domain Name Server (DNS) software package from the Internet Systems Consortium (ISC) commonly used to resolve host names to IP addresses and vice versa. As a key element in the Internet's infrastructure, DNS servers have often been targets of attack by hackers, spammers and phishers. By taking a few simple steps, you, the customer, can help protect your networks and help protect the Internet as well.

- Date: 02/14/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/bind-9-dns-security.cfm
- Category: IA Guidance > Security Configuration > Applications
- SHA256: 22059B8076D4038980C85FE2D6F8D80BA3D30902809B5AFDC4971276E5A43EEA
- Size: 225KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Unified Communications Technical Primer

- Abstract: The purpose of this fact sheet is to provide IT managers with a brief introduction to Unified Communications (UC) and the technologies that make up UC. This fact sheet should be used as a starting point for IT managers who are researching whether to upgrade their current infrastructure to incorporate a UC solution. Once they make the decision to implement UC, they should follow recommendations from NSA's IA Guidance for UC Deployments document.
- Date: 01/03/2011
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/unified-communications-technical-primer.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 7EF6C440EAE5CBDB93F469C75670D9484CC8D560260E7864DBDA98EC2EF8537E
- Size: 433KB
- Location: Archive

- Access Controlled: False

Return to the Table of Contents.

Security Highlights of Windows 7

- Abstract: This guide highlights many of the new security features in Windows 7, just one of the many commercial operating systems available.
- Date: 10/06/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/security-highlights-of-windows-7.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: 2F6C108733A3A5E95E1EA7D17A1A9D821C1902CBD57DC3EF381DEFF7AD740364
- Size: 412KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Securing Lotus Sametime

- Abstract: This guide has been designed to provide a high-level security reference when deploying a Sametime solution. It is intended to be utilized in parallel with the security features already present in Lotus Domino and Sametime. There are many configurations for a Sametime deployment. Depending on the feature set desired, the environment can become complex. It is important to implement security throughout the deployment process and work out any bugs along the way. Successfully securing your Sametime environment can save time, money, and help protect your sensitive information from today's most common threats.
- Date: 09/22/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/securing-ibm-lotus-sametime.cfm

- Category: IA Guidance > Archive
- SHA256: BBF6D32B1003EBA0F359A4DA59459DF836C70388C80A4A239CE72167755A67FF
- Size: 494KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

A Framework for Assessing and Improving the Security Posture of Industrial Control Systems

- Abstract: This publication is the first in a series intended to help Industrial Control System (ICS) owners and operators in need of improving the security posture of their systems. This document will focus the reader on aspects of network security and give them a framework for assessing their current operational risk. It will then offer the reader a quantifiable approach to help them make decisions for reducing risk and improving their systems security posture.
- Date: 08/20/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/a-framework-for-assessing-and-improving-the-security-posture.cfm
- Category: IA Guidance > Security Configuration > Industrial Control Systems
- SHA256: 4881083C3975EF44A16B556B70CE4E9030C35969EC5156C8364FF43FFBA45407
- Size: 936KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Microsoft Office 2003

- Abstract: This Inspection and Sanitization Guidance for Microsoft Office 2003 document provides guidance and specifications for developing file inspection and sanitization software for Microsoft Office 2003 files (i.e., word processing, presentation, and spreadsheet documents).
- Date: 08/17/2010
- Link: https://apps.nsa.gov/iaarchive/library/reports/ms_office_2003_inspection_and_sanitization_guidance_v1_0_2-20171212.cfm
- Category: Reports
- SHA256: 1F6B0EFBFA78E9AACFCE9BD48AB061C75E9200DCB851C0D5F069EDE09B84F36E
- Size: 1,070KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Cisco Unified Presence Server

- Abstract: This document goes over Cisco Unifed Presence Server (CUPS) and what it is, the functions, risks, etc.
- Date: 08/01/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/cups.cfm
- Category: IA Guidance > Archive
- SHA256: D73CF95F6B46F8852258AFAC99268F1B6317EDEDCA43B2A15E177A62BF51F33C
- Size: 535KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Whitelisting using Software Restriction Policies

- Abstract: Software Restriction Policies (SRP) enables administrators to control which applications are allowed to run on Microsoft Windows. SRP is a feature of Windows XP and later operating systems. It can be configured as a local computer policy or as domain policy using Group Policy with Windows Server 2003 domains and later. Using this guide, administrators can configure SRP to prevent all applications in their domain from running except applications they explicitly allow. Utilizing SRP as an application whitelisting technique significantly increases the security posture of the domain by preventing many malicious programs from executing.
- Date: 08/01/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/operating-systems/application-whitelisting-using-srp.cfm
- Category: IA Guidance > Security Configuration > Operating Systems
- SHA256: 3194220BFBF72D090512A55194F3FEA5927A914D2F2969A631482EB4A8F418B5
- Size: 385KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Application Whitelisting

- Abstract: This document provides an overview of Application Whitelisting, including what it is, why one should use it, and how to enforce it.
- Date: 08/01/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/application-whitelisting-trifold.cfm
- Category: IA Guidance > Archive
- SHA256: 2F2797B6D84D42A57B67DB86BB982E96AA2822E61D83B50DD84C004D661E523F
- Size: 543KB

- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Inspection and Sanitization Guidance for Microsoft Office 2007 and Office Open XML (OOXML)

- Abstract: This Inspection and Sanitization Guidance for Microsoft Office 2007 document provides guidance and specifications for developing file inspection and sanitization software for Microsoft (MS) Office 2007 files (i.e., word processing, presentation, and spreadsheet documents). Client programs, such as MS Office Word 2007, can store arbitrary data in a MS Office 2007 document, including video, sounds, and hidden text. This presents a challenge for automated file processing software. This document addresses this challenge by delineating the various constructs with the Office 2007 file formats. The document provides specific guidelines for designing, building, and testing Office 2007 file inspection and sanitization applications.
- Date: 06/18/2010
- Link: https://apps.nsa.gov/iaarchive/library/reports/ms_office_2007_inspection_and_sanitization_guidance_v1_0-20171212.cfm
- Category: Reports
- SHA256: 00B28829861B994B42498600CC1FE1BCF40A157298BCF597E2F3809D502732B4
- Size: 1,222KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Activating Authentication and Encryption for Cisco Unified Communications Manager Express 7.0/4.3

- Abstract: The intent of this document is to provide step-by-step instructions for configuring authentication and encryption for Cisco Unified Communications Manager Express (CUCME) releases 4.2, and 7.0/4.3.

- Date: 04/28/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/activating-authentication-and-encryption-for-cucme-7-0-4-3.cfm
- Category: IA Guidance > Archive
- SHA256: B7782E4DDAC357260E8BDE828BE9DB363F6EE7EFA971AA8A656C01B473CEA537
- Size: 551KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Mathematical routines for the National Institute of Standards and Technology prime elliptic curves

- Abstract: Described in this document are routines for implementing primitives for elliptic curve cryptography on the NIST elliptic curves P–192, P–224, P–256, P–384, and P–521 given in [FIPS186-2]. Also included are specialized routines for field arithmetic over the relevant prime fields and example calculations.
- Date: 04/05/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/mathematical-routines-for-the-nist-prime-elliptic-curves.cfm
- Category: IA Guidance > IA Solutions For Classified > Algorithm Guidance
- SHA256: EC51030A4E577C059B27F47A6B2727DCFA45D1B886F4C8BA5FA70E3793FE4AD6
- Size: 205KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Host and Network Integrity through Trusted Computing

- Abstract: This document provides an overview of the Trusted Computing Group including explaining the Trusted Platform Module, Measured Boot and Measured Launch, Network Access Control, Recommendations, and Host Integrity at Startup.
- Date: 04/01/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/host-networking-integrity-through-trusted-computing.cfm
- Category: IA Guidance > Technical Briefs
- SHA256: 5394CE51F4D7AFC3F8F4326736F30FF7CCB5508F09E37E87CD52BB7DF33A016E
- Size: 560KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Defense in Depth

- Abstract: This paper provides an overview of the major elements of the strategy and provides links to resources that provide additional insight.
- Date: 03/12/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm
- Category: IA Guidance > Archive
- SHA256: C7DE6ACB92CBFFCF387AE9F055CE5F54C178F51A2FC6F58F74DF73C44534E9E0
- Size: 670KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Hardening Tips for Mac OS X 10.6 Snow Leopard

- Abstract: This trifold contains, in order of importance, high-impact tips designed for use by an administrative user of Mac OS X 10.6 Snow Leopard.
- Date: 03/01/2010
- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/hardening-tips-for-mac-os-x-10-6-snow-leopard.cfm
- Category: IA Guidance > Archive
- SHA256: 06298E5A8A5DFB780C5CF771B8F318D835CD59C1C512250897E3659A0D1CF021
- Size: 485KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.

Suite B Implementer's Guide to Federal Information Processing Standard 186-3

- Abstract: This document specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) from the "Digital Signature Standard" [FIPS186-3] that will be used in future and existing cryptographic protocols for Suite B products. It also includes the Suite B elliptic curve domain parameters, (NIST curves P-256 and P-384), along with example data for the ECDSA signature algorithm on these curves and auxiliary functions that are necessary for ECDSA implementations to be in compliance with [FIPS186-3] and Suite B. [FIPS186-3] defines methods for digital signature generation that can be used for the authentication of binary data (commonly called a message), and for the verification and validation of those digital signatures. One of the approved techniques is the Elliptic Curve Digital Signature Algorithm (ECDSA) but additional requirements are specified. This document includes requirements for obtaining the assurances necessary for valid digital signatures. Methods for obtaining these assurances are provided in the NIST Special Publication [SP800-89].
- Date: 02/03/2010

- Link: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/suite-b-implementers-guide-to-fips-186-3-ecdsa.cfm
- Category: IA Guidance > IA Solutions For Classified > Algorithm Guidance
- SHA256: A27A08A1A76DB19109BD014CE172DC09B2184FDBE3B049E3DA0816312646032A
- Size: 177KB
- Location: Archive
- Access Controlled: False

Return to the Table of Contents.
