tyco | Software House

C•CURE 9000 and iSTAR Cybersecurity Overview

White Paper

Version 2.0

C•CURE 9000 v2.80

iSTAR v6.7

February 2020

Johnson Controls

Introduction

C•CURE 9000 provides peace of mind to our customers with a holistic cyber mind-set beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guaranty that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Executive summary

C•CURE 9000 and the iSTAR panels are versatile and secure Johnson Controls access control products. Adopted by government and critical infrastructure sites, financial, medical, and education institutes, C•CURE 9000 and the iSTAR panels have many certifications and security audits.

The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge control panels has achieved FIPS 140-2 and FIPS 197 validation. When in FIPS-approved or “dark” mode, the iSTAR panels disable all access except direct communications from C•CURE 9000.

Both C•CURE 9000 and the iSTAR panels are developed under a Secure Development Life Cycle that includes secure coding techniques, strict source code control, regular vulnerability and penetration testing, and vulnerability management. When vulnerabilities are discovered after deployment, the cross-functional Cyber-Response team can provide a response the same day.

C•CURE 9000 and the iSTAR panel offer a secure platform that you can customize to meet the security policies of almost any installation and comes with a dedicated support team to address vulnerabilities and other security issues as they arise. This document serves to answer many of the frequently asked cybersecurity questions and identify some of the many security features available in C•CURE 9000 and the iSTAR panels. If questions or issues do arise, contact your Software House representative.

Contents

Introduction 2

Legal disclaimer 3

Executive summary 4

The C•CURE 9000 system 8

- Architecture overview 8
- Enterprise architecture 9
- Microsoft Windows operating system 9

Robustness 10

- Backup/Restore 10

Access control 10

- Authentication 10
- Separation of responsibilities 11

Communication protection 12

- C•CURE 9000 12
- iSTAR 13

iSTAR operating system 14

- Firmware updates 14

iSTAR database 15

Tamper detection 15

Security approvals and certifications 16

- FISMA 16
- FICAM FIPS-201 certified/GSA approved products lists 16
- FIPS 197 17
- FIPS 140-2 17

APPENDIX – Resources and references 18

- Johnson Controls documents 18
- Laws and regulations 18
- OMB circulars 18
- FIPS publications 18
- NIST publications 18

Our Product Security Program: Firmly established, always evolving. Johnson Controls creates products and solutions in a culture focused on cyber resilience and we deploy with dedicated support. Our customers benefit from our proven approach:

- Consistent, organization-wide focus.
- Time-tested policies and practices.
- Global knowledge base.
- Support from design through deployment and beyond.
- Continuing investment to meet ever-evolving challenges and needs.

Structured methodology – Because disruption is not an option

Your facility's systems are crucial to continuing operations and maintaining profitability. Johnson Controls takes a holistic, structured approach to help you protect systems and sensitive data from the risk of a cyber-attack.

Disciplined governance. Our Product Security Team employs global governance to put cyber resilience at the forefront. We pursue and continually improve a disciplined, policy-driven approach.

Expert-driven design. Engineering teams are trained in cybersecurity and in designing solutions that support compliance. Cybersecurity experts with certifications including, CISSP, CSSLP, CEH, and CCSP validate designs using up-to-the-minute best practices.

Security-infused development. We work to uncover, remediate and protect against concerns long before product release, through in-house testing that includes the integration of security tooling throughout the development lifecycle.

Knowledge-driven deployment. Through customer education, compliance assistance, security documentation, and our pragmatic approach, we help to facilitate more secure installation.

Lifecycle management. Cybersecurity continues to change, so our security approach goes beyond development and deployment to address tomorrow's concerns as they arise.

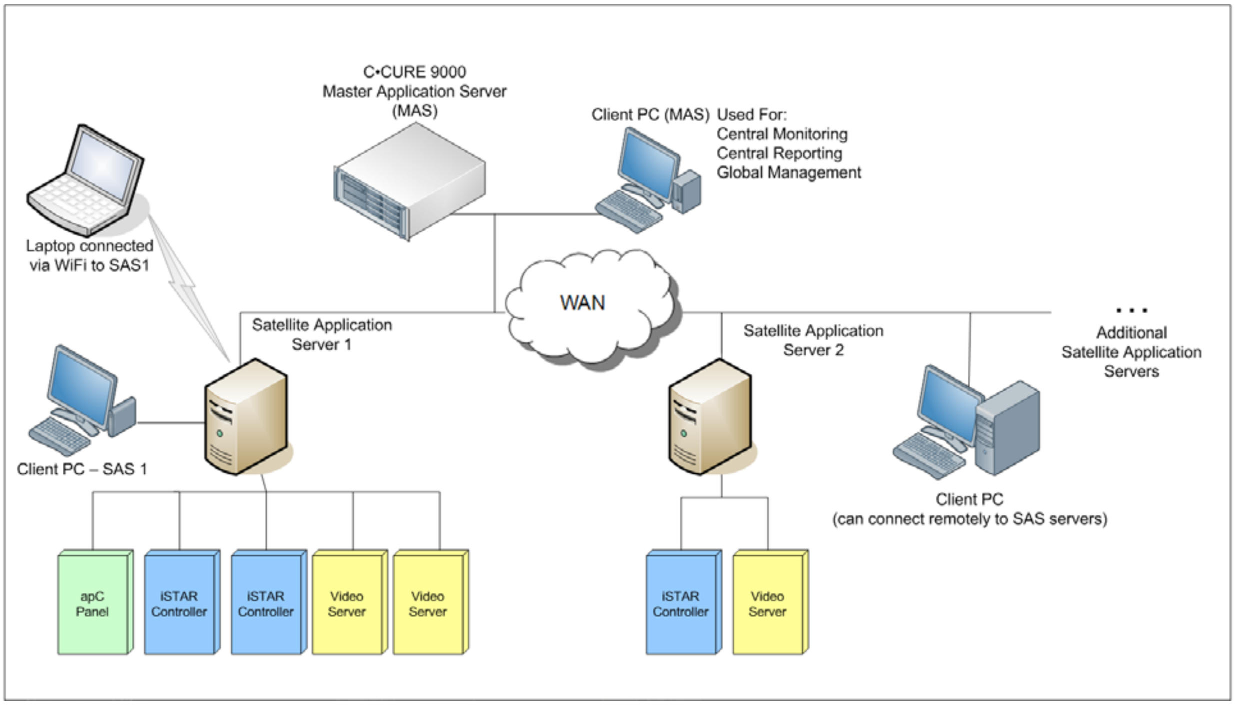
Rapid response. Our dedicated cybersecurity team emphasizes speed, transparency and professionalism. We monitor trends, assess new threats and provide guidance on handling vulnerabilities and reducing exposure.

Commitment to partnership. Johnson Controls is dedicated to sharing your responsibility for more secure systems. We support you through education, engagement and thought leadership for greater success in achieving your mission.

The C•CURE 9000 system

Architecture overview

Figure 1



C•CURE 9000 is a flexible, object-oriented security and event management system that features a variety of customizable interfaces for maintaining the system, and for monitoring the sites that you want to secure.

C•CURE 9000 provides extensive information management capability using Microsoft SQL Server and Microsoft .NET Framework V4.6.1. Its distributed client-server architecture is capable of supporting a large array of clients, controllers, and input devices, including various card readers and cameras.

C•CURE employs two thick clients. The Administration Station manages the customized C•CURE 9000 functions, objects, and views of the Monitoring Station. The Monitoring Station tracks events and status of devices, and can control manual actions such as locking and unlocking doors, depending on configuration and operator privileges.

The iSTAR panels are the hardware controllers that interface with access control card readers, locks, and other physical security hardware. They may be configured into clusters with a single master controller communicating to the iSTAR host and store a local version of the access control database so they can continue to operate during a network failure.

Enterprise architecture

C•CURE 9000 Enterprise Architecture is a licensable option that allows you to configure multiple C•CURE 9000 servers to communicate with a Master Application Server (MAS). MAS provides a platform for global management of the Personnel, Video, and access security objects on two or more Satellite Application Servers (SAS) in an enterprise system.

MAS contains the global data that is used across every server, such as global Personnel records, global Clearances, and global Operators. The global data is synchronized to each SAS so that it can be used to implement enterprise-wide security.

The MAS itself does not have any directly connected controllers or video servers, but it can be used to remotely monitor and manage controllers and video servers attached to SAS machines in the enterprise. The MAS provides the capability for Central Monitoring of the entire enterprise, using the C•CURE 9000 Monitoring Station application. You can view Events, Activities, and status of each SAS in the enterprise from a central Monitoring Station connected to the MAS. Alternatively, you can connect to a particular SAS to monitor that system and its connected hardware. In addition, the MAS provides a Central Reporting capability, because its database includes information about all objects that are replicated from the satellite servers.

Each Satellite Application Server contains database records for the video and access security hardware connected to it, in addition to local personnel, clearances, privileges, and other data. Each SAS synchronizes with the MAS so that SAS local data is replicated to the MAS for central management and monitoring.

All data is synchronized immediately when saved (or queued if a server is offline), except for Journal and Audit data, which is synchronized on a configurable schedule.

Note: Network latency and load on the MAS and SAS databases can affect synchronization performance.

Operator Privileges are used to provide system users with access to the information they need, and deny access to information they do not need or should not be able to view.

These capabilities let you deploy multiple C•CURE 9000 servers in an enterprise environment, solving scalability and wide area network issues and providing a platform for central monitoring, global management, and central reporting.

Microsoft Windows operating system

The licensed capabilities of C•CURE 9000 corresponds to the specific version of the Windows operating system it is installed upon. As the host environment, Windows provides the underlying foundation for configuring a secure C•CURE 9000 system. Tools such as Microsoft Security Configuration Manager, Security Compliance Manager and Windows domain policies can be used to optimize the security of the system.

Additionally, the roles and responsibilities assigned to each C•CURE 9000 user is dependent on the specific Windows operator. This allows user credentials and access to the system to be controlled through Windows Active Directory.

Robustness

Backup/Restore

C•CURE 9000 uses three databases that you can back up at any time using the System Backup feature.

- The Core database is a core component of the management platform upon which C•CURE 9000 is built. It is the central repository for configuration details describing objects created, monitored, and maintained in C•CURE 9000.
- The Audit Log provides a history of changes to configurations managed by C•CURE 9000.
- The Activity Journal maintains a record of activity monitored by the system. Records in the Activity Journal provide a historical view of activity that has occurred within the system, statistical information on resource usage, and personnel and asset location information.

In the event of a system failure or corruption of the Core, Audit Log or Activity Journal database, you can restore one or more of these databases from a backup of the respective database.

The C•CURE 9000 Server Configuration Application Guide describes the details for performing system backup and restore.

User access to the System Backup feature is controlled through the user configuration.

Access control

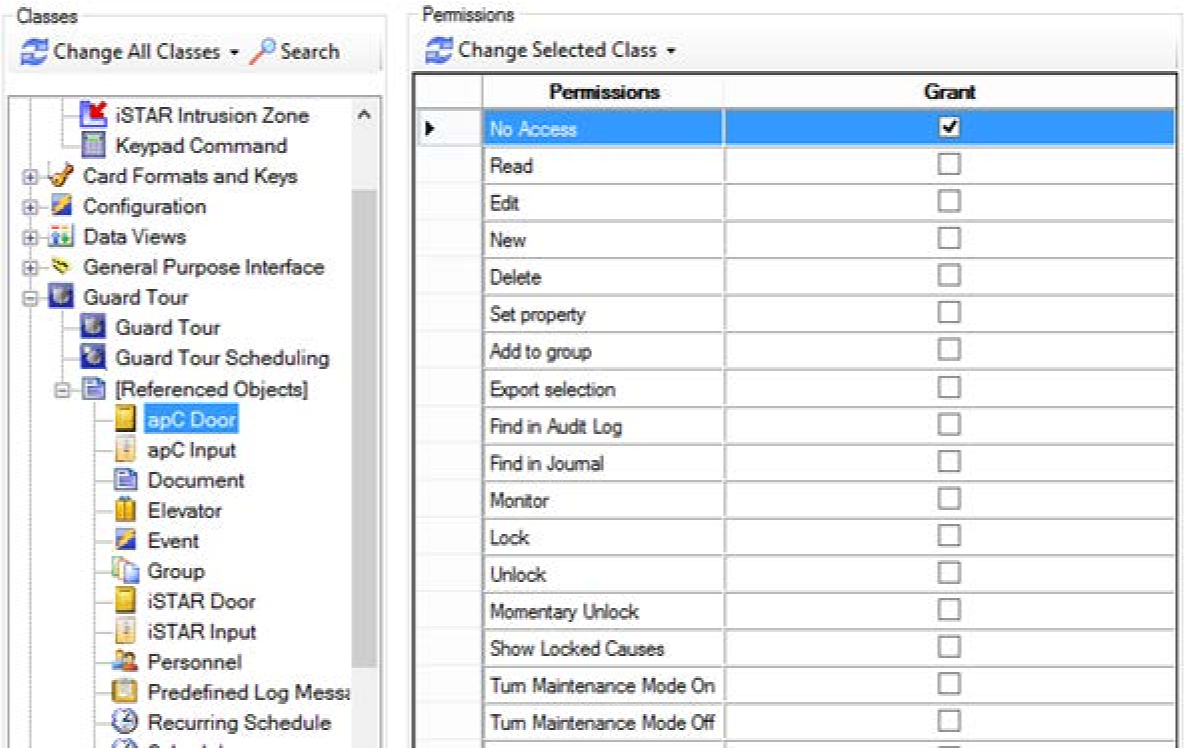
Authentication

C•CURE 9000 is designed for deployment in an Active Directory domain environment utilizing Windows Single Sign-On (SSO) to integrate login credentials with operator permissions. This provides a seamless user authentication and authorization process. Password rules and policies such as predefined number of login attempts, character length, combination of alpha numeric, and user-defined lockouts are managed by the local Microsoft Windows operating system or the domain controller. C•CURE 9000 does not store or have any visibility of the credentials.

Separation of responsibilities

C•CURE 9000 has highly configurable operator privilege functionality. Using the Privilege Editor feature, administrators can specify the objects, programs, reports, Personnel, events, and actions that Operators can view and use. The feature also allows for exceptions and bulk configuration.

Figure 2

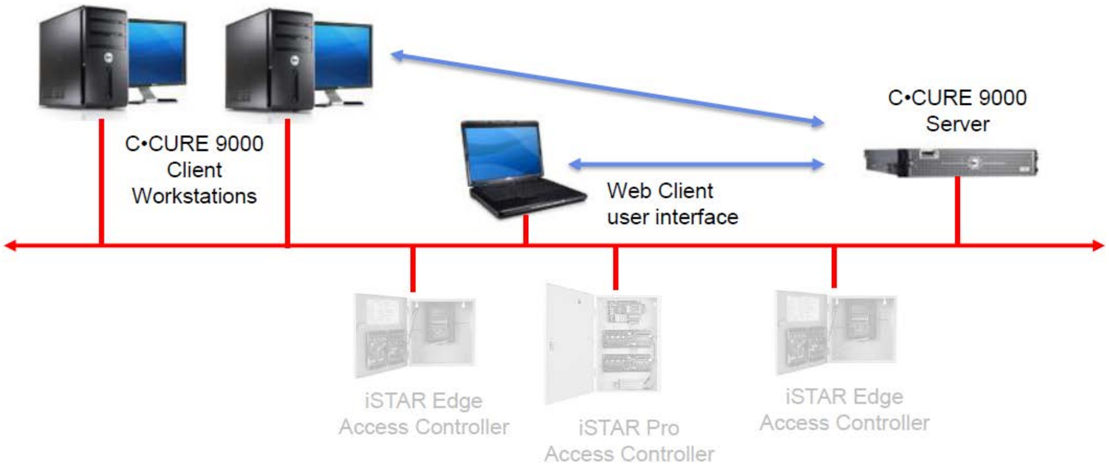


Permissions	Grant
No Access	☑
Read	☐
Edit	☐
New	☐
Delete	☐
Set property	☐
Add to group	☐
Export selection	☐
Find in Audit Log	☐
Find in Journal	☐
Monitor	☐
Lock	☐
Unlock	☐
Momentary Unlock	☐
Show Locked Causes	☐
Turn Maintenance Mode On	☐
Turn Maintenance Mode Off	☐

Communication protection

C•CURE 9000

Figure 3



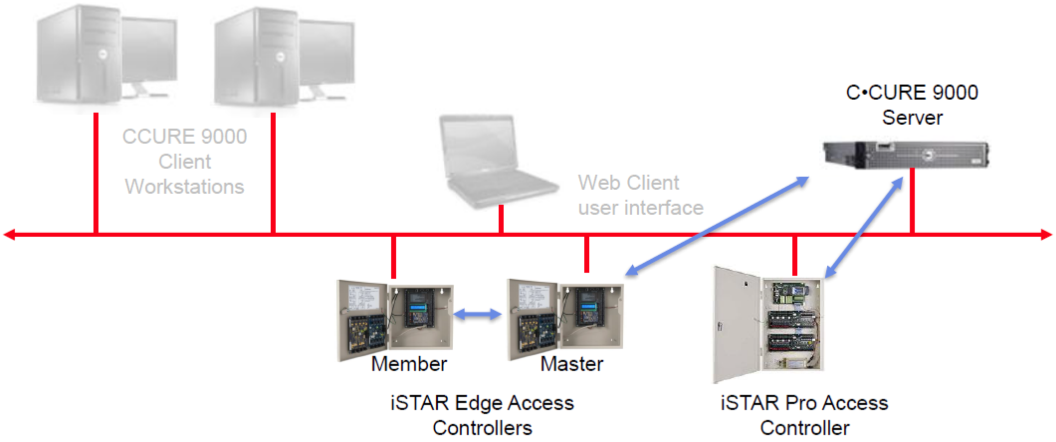
Communication between the C•CURE 9000 server, iSTAR controller, database, or client devices uses the Crossfire service. By default, the CrossFire server uses AES-256 encryption that has been FIPS 197 validated.

(Line 2857): http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html

iSTAR

In standard mode, the iSTAR Edge and iSTAR Ultra use TLS to communicate securely with the host and other cluster members. The encryption is FIPS 197 listed (AES 256).

Figure 4



In FIPS mode, the iSTAR will use TLS to authenticate the controller to the C•CURE 9000 host. The system may be set up to use a default certificate, or it may be set up to use a custom certificate provided by a third-party or auto-generated by the C•CURE 9000 host.

- Controller-Based Encryption Mode – C•CURE 9000 creates the Host and CA certificates at the C•CURE 9000 host computer and then directs the iSTAR encrypted controller to generate new public and private keys.
- Host Based Encryption Mode – C•CURE 9000 creates the Host, Controller, and CA certificates on the host computer and then downloads the Controller public key, the Controller private key and the CA certificate to the iSTAR controller. Host-Based Encryption allows the use of a certificate created by a third-party certificate authority.

The default asymmetric encryption is RSA 1024, but may be changed to ECC 571 at the cluster level. The symmetric key remains AES 256.

The iSTAR Edge and iSTAR Ultra are tested and listed for FIPS 140-2 level 2 for cryptographic modules:

- iSTAR Edge: FIPS 140-2 certificate #2309
- iSTAR Ultra: FIPS 140-2 certificate #2315

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Also, in FIPS approved mode, the iSTAR controller disables all ports except those required for communication between the C•CURE 9000 host and other iSTARs in FIPS approved mode. It only accepts communication from the C•CURE 9000 host and the iSTARs in its cluster.

The iSTAR Ultra family supports TLS v1.2 only at minimum.

iSTAR operating system

The iSTAR Ultra family operating systems are Linux-based.

The embedded web server has been developed internally and may be turned off through the controller’s setup screen.

Firmware updates

Firmware downloads are issued from the Monitoring Application or a separate utility called ICU utilizing TCP port 1999. The panel continues to operate during the firmware download process. When the panel receives the proper check-sum, this signifies a successful download. The controller must reboot when a successful download is completed. After a successful reboot the server re-establishes communication issuing a fresh personnel and configuration download to the panel. If the panel does not receive the proper checksum then the panel continues to use the previously stored firmware.

iSTAR database

The iSTAR downloads three specific data sets that allow it to operate and make access control decisions: cardholder data, configuration data, and firmware. When a controller is first placed online, the C•CURE 9000 iSTAR driver downloads all pertinent data to that panel. The fast personnel download and the configuration download take place at this time. The fast personnel download uses TCP port 2801. It creates a single file of all personnel data that have access privileges to any of the doors associated with the panel being placed online. All additional incremental system changes regarding cardholder or hardware configurations get downloaded in real-time. Major personnel changes implemented at the server cause the system to perform a fast personnel download to the panels that are affected.

By default the database on the iSTAR is encrypted with AES 256. However, if additional security is required, activating the CPNI mode on the iSTAR Ultra prevents the database from being stored in persistent memory.

ICU now redirects requests to edit any controller configuration setting such as IP address or Host IP, or downloading firmware back to the controller’s local web page where editing can take place in a much more secure environment.

The web diagnostics user interface on the iSTAR provides the option to encrypt the main partition of the SD card (OS, access control FW, and customer DB). After the encryption process is finished, the panel boots up normally and continues operation without delay or configuration loss. And in C•CURE 9000 v2.80, you can display the Encrypted Status of each panel. Note that a unique key is used for encryption, so it is no longer be possible to change just the SD card on an iSTAR Ultra.

Enforced unique, strong password, for each controller, for the web diagnostics page. Web passwords must be changed upon initial controller boot up, and, you can change and manage this centrally through C•CURE 9000 v2.80.

Tamper detection

All iSTARs include tamper detection. If the enclosure has been opened an alarm is activated. The iSTAR Ultra includes an optional installation of a back tamper it case it is removed from the wall.

iSTAR Ultra and iSTAR Edge have been FIPS 140-2 approved to provide physical protection of the encryption module. This includes the metal enclosure, physical tamper, preventing visibility, and using tamper evident labels.

Security approvals and certifications

FISMA

You can configure the C•CURE 9000 system to support the controls necessary for overall FISMA compliance. These controls include:

- Authenticated system access.
- Account login/logout management.
- Role-based separation of capabilities, permissions, and privileges.
- System event and configuration change auditing, alerting, and management.
- Restriction of ports, protocols, and services to only those required to support C•CURE 9000 functionality.
- Encrypted communications.

FICAM FIPS-201 certified/GSA approved products lists

The Software House C●CURE 9000 has been tested and certified as an end-to-end physical access control system with high assurance readers and validation software. The system has been tested and approved as a fully compliant FICAM Solution by the U.S. General Services Administration. The approval means that the C•CURE 9000, high assurance readers and validation software meet the rigorous testing requirements and comply with the FICAM roadmap and the realignment of the GSA's Approved Product List (APL). The system was subjected to numerous tests to ensure that the system is not prone to denial of service, credential spoofing, or other types of unauthorized access that could compromise the security of the system. C•CURE 9000 provides a solution for HSPD-12 / FIPS-201 and 800-116 compliance for smart card credentials, along with support for PIV-I, PIV-C, TWIC and the DOD CAC credential using authentication software with its Server-based Certificate Verification Protocol (SCVP) client.

FIPS 197

C•CURE 9000 and the iSTAR Controllers have been certified by the NIST CMVP as meeting the requirements of FIPS 197 AES encryption algorithm standard.

FIPS 140-2

The C•CURE 9000 iSTAR Edge and Ultra controller models have been certified by the NIST CMVP as meeting the requirements of FIPS 140-2 Level 2.

APPENDIX – Resources and references

Johnson Controls documents

The following documents are available at https://www.johnsoncontrols.com/cyber-solutions

- C•CURE 9000/iSTAR Port Assignments
- C•CURE 9000/iSTAR FISMA-Ready Compliance Guide
- C•CURE 9000 v2.80/iSTAR NERC-CIP v6 Compliance Guide

Laws and regulations

- Federal Information Security Management Act of 2002
- Federal Information System Modernization Act of 2014
- Consolidated Appropriations Act of 2005, Section 522.
- USA PATRIOT Act (P.L. 107-56), October 2001.

OMB circulars

- OMB Circular A-130, Management of Federal Information Resources, November 2000.
- OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June, 2006.

FIPS publications

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems

NIST publications

- NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST 800-30, Risk Management Guide for Information Technology Systems
- NIST 800-34, Contingency Planning Guide for Information Technology Systems

- NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations
- NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
- NIST 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security
- NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
- NIST 800-64, Security Considerations in the Information System Development Life Cycle
- Framework for Improving Critical Infrastructure Cybersecurity