# Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous FISMA Compliance

Draft 1.0: February 23, 2009

*NOTICE to readers of this draft document:  Criticisms and suggestions are strongly encouraged. If you are actively engaged in cyber forensics, red teams, blue teams, technical incident response, vulnerability research, or cyber attack research or operations, please help make sure this document is as good as it can be.  We also request support in identifying users who have implemented scalable methods for measuring compliance with these controls and producing sharable benchmarks and other types of baseline guidance that can be used to drive tool-based assessment of as many of these controls as possible.*

*Send criticism/comments/suggestions to John Gilligan <jgilligan@gilligangroupinc.com> as well as to cag@sans.org by March 25, 2009.*

## INTRODUCTION

Securing our Nation against cyber attacks has become one of the Nation's highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks.  Furthermore, for those external attacks that are successful, defenses must be capable of thwarting, detecting, and responding to follow-on attacks on internal networks as attackers spread inside a compromised network.

A central tenet of the US Comprehensive National Cybersecurity Initiative (CNCI) is that 'offense must inform defense'. In other words, knowledge of actual attacks that have compromised systems provides the essential foundation on which to construct effective defenses.  The US Senate Homeland Security and Government Affairs Committee moved to make this same tenet central to the Federal Information Security Management Act in drafting FISMA 2008. That new proposed legislation calls upon Federal agencies to:

> *"Establish security control testing protocols that ensure that the information infrastructure of the agency, including contractor information systems operating on behalf of the agency, are effectively protected against known vulnerabilities, attacks, and exploitations."*

And to work together to make sure that testing is up to date and comparable, by agreeing on common metrics through:

> *"Establishing a <u>prioritized baseline</u> of information security measures and controls that can be continuously monitored through automated mechanisms."*

This consensus document is designed to begin the process of establishing that *prioritized baseline of information security measures and controls*.  The consensus effort that has produced

this document has identified twenty specific security controls that are viewed as essential for blocking known high-priority attacks.  Fifteen of these controls can be monitored, at least in part, automatically and continuously.  The consensus effort has also identified a second set of five controls that are essential but that do not appear to be able to be monitored continuously or automatically with current technology and practices.

Additionally, the controls in this document are designed to support agencies and organizations that currently have various different levels of information security capabilities.  To help organizations focus on achieving a sound baseline of security and then improve beyond that baseline, certain aspects of individual controls have been categorized as follows:

- *Quick Wins:* These fundamental aspects of information security can help an organization rapidly improve its security stance generally without major process, organization, architecture, or technical changes to its environment.  It should be noted, however, that a *Quick Win* does not necessarily mean that these controls provide protection against the most critical attacks.  The intent of identifying *Quick Win* control areas is to highlight where security can be improved rapidly. These items are identified in this document with the label of "QW."
- *Improved Visibility and Attribution:* These controls focus on improving the process, architecture, and technical capabilities of organizations so that the organization can monitor their networks and computer systems, gaining better visibility into their IT operations.  Attribution is associated with determining which computer systems, and potentially which users, are generating specific events.  Such improved visibility and ability to determine attribution supports organizations in detecting attack attempts, locating the points of entry for successful attacks, identifying already-compromised machines, interrupting infiltrated attackers' activities, and gaining information about the sources of an attack.  These items are labeled as "Vis/Attrib."
- *Hardened Configuration and Improved Information Security Hygiene:* These aspects of various controls are designed to improve the information security stance of an organization by reducing the number and magnitude of potential security vulnerabilities as well as improving the operations of networked computer systems.  Control guidelines in this category are formulated with the understanding that a well-managed network is a much harder target for computer attackers to exploit.  Throughout this document, these items are labeled as "Config/Hygiene."
- *Advanced:* These items are designed to further improve the security of an organization beyond the other three categories. Organizations handling particularly sensitive networks and information that are already following all of the other controls should focus on this category.  Items in this category are simply called "Advanced."

In general, organizations should examine all twenty control areas against their current status and develop an agency-specific plan to implement the controls.  Organizations with limited information security programs may want to address the "Quick Wins" aspects of the controls in order to make rapid progress and to build momentum within their information security

program.  On the other hand, controls identified as Advanced would typically be implemented to augment or extend controls in the other three categories of controls.

**Why This Project Is So Important: Gaining Agreement among CISOs, CIOs and IGs**

Federal Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) are charged with improving the state of information security across the Federal government.  Moreover, they are spending increasing amounts of money to secure their systems.  However, the complexity of securing their systems is enormous, and therefore there is a need to focus attention and resources on the most critical risk (and therefore the highest payoff) areas.  In addition, CISOs and CIOs want and need specific guidance that can be consistently applied and upon which their performance in improving security can be consistently and fairly evaluated.  At the same time, Federal Inspectors General (IGs) and auditors want to ensure that CIOs and CISOs are doing what is necessary to secure systems, but IGs and auditors, too, need specific guidance on how to measure security.

This document is a first step toward providing specific audit guidelines that CISOs, CIOs, IGs, and the US-CERT can adopt to ensure their agency systems have the baseline security controls in place that are most critical.  It takes advantage of the knowledge gained in analyzing the myriad attacks that are being actively and successfully launched against federal systems and our nation's industrial base systems and identifying the key controls that are most critical for stopping those attacks.  This effort also takes advantage of the success and insights from the development and usage of standardized concepts for identifying, communicating, and documenting security-relevant characteristics/data.  These standards include the following: common identification of vulnerabilities (Common Vulnerabilities and Exposures—CVE), definition of secure configurations (Common Configuration Enumeration-CCE), inventory of systems and platforms (Common Platform Enumeration-CPE), vulnerability severity (Common Vulnerability Scoring System-CVSS) and identification of application weaknesses (Common Weaknesses Enumeration-CWE). These standards have emerged over the last decade through collaborative research and deliberation between government, academia and industry.  While still evolving, several of these efforts in standardization have made their way into commercial solutions and government, industry, and academic usage.  Perhaps most visible of these has been the Federal Desktop Core Configuration (FDCC) which leveraged the Security Content Automation Program (SCAP). SCAP utilizes mature standardization efforts to clearly define common security nomenclature and evaluation criteria for vulnerability, patch, and configuration measurement guidance and is intended for adoption by automated tools.  It is strongly recommended that automated tools used to implement or verify security controls identified in this document employ SCAP or similar standardization efforts for clearly defined nomenclature and evaluation criteria not covered by SCAP.  Additional areas of standardization are emerging (e.g., application weaknesses, events, malware attributes, attack patterns, remediation actions) that in the future will be of benefit for some of the controls identified in this document.

The National Institutes of Standards and Technology (NIST) has produced excellent security guidelines that provide a very comprehensive set of security controls. This document by contrast seeks to identify that subset of security control activities that CISOs, CIOs and IGs can agree are their top, shared priority for cyber security. Once agreement is reached, these controls would be the basis for future audits and evaluations. While aimed at government organizations, the principles and measures addressed in this document are also highly applicable to commercial and academic enterprises and should be usable within the commercial marketplace.

What makes this document effective is that it reflects knowledge of actual attacks and defines controls that would have stopped those attacks from being successful. To construct the document, we have called upon the people who have first-hand knowledge about how the attacks are being carried out:

1. Red team members in NSA tasked with finding ways of circumventing military cyber defenses
2. Blue team members at NSA who are often called in when military commanders find their systems have been compromised
3. US-CERT and other non-military incident response employees and consultants who are called upon by civilian agencies and companies to identify the most likely method by which the penetrations were accomplished
4. Military investigators who fight cyber crime
5. Cybersecurity experts at US Department of Energy laboratories and Federally Funded Research and Development Centers (FFRDCs).
6. DoD and private forensics experts who analyze computers that have been infected
7. Civilian penetration testers who test civilian government and commercial systems to find how they can be penetrated
8. Federal CIOs and CISOs who have intimate knowledge of cyber attacks
9. The Government Accountability Office (GAO)

**Consensus Audit Guideline Controls**

Twenty critical security controls were agreed upon by knowledgeable individuals from the groups listed above. The list of controls includes fifteen that are able to be validated in an automated manner and five that must be validated manually.

Critical Controls Subject to Automated Measurement and Validation:

1: Inventory of Authorized and Unauthorized Hardware.
2: Inventory of Authorized and Unauthorized Software.
3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.
4: Secure Configurations of Network Devices Such as Firewalls and Routers.
5: Boundary Defense

6: Maintenance and Analysis of Complete Security Audit Logs
7: Application Software Security
8: Controlled Use of Administrative Privileges
9: Controlled Access Based On Need to Know
10: Continuous Vulnerability Testing and Remediation
11: Dormant Account Monitoring and Control
12: Anti-Malware Defenses
13: Limitation and Control of Ports, Protocols and Services
14: Wireless Device Control
15: Data Leakage Protection

Additional Critical Controls (not directly supported by automated measurement and validation):

16. Secure Network Engineering
17. Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Training to Fill Gaps

In the pages that follow, each of these controls is described more fully. Descriptions include how attackers would exploit the lack of the control, how to implement the control, and how to measure if the control has been properly implemented, along with suggestions regarding how standardized measurements can be applied. As pilot implementations are complete and agencies get experience with automation, we expect the document to be expanded into a detailed audit guide that agency CIOs can use to ensure they are doing the right things for effective cyber defense and that IGs can use to verify the CIOs' tests.

**Insider Threats vs. Outsider Threats**

A quick review of the critical controls may lead some readers to think that they are heavily focused on outsider threats and may, therefore, not fully deal with insider attacks. In reality, the insider threat is well covered in these controls in two ways. First, specific controls such as network segmentation, control of administrative rights, enforcement of need to know, data leakage protection, and effective incident response all directly address the key ways that insider threats can be mitigated. Second, the insider and outsider threats are merging as outsiders are more and more easily penetrating the security perimeters and becoming "insiders." All of the controls that limit unauthorized access within the organization work effectively to mitigate both insider and outsider threats. It is important to note that these controls are meant to deal with multiple kinds of computer attackers, including but not limited to malicious internal employees and contractors, independent individual external actors, organized crime groups, terrorists, and nation state actors, as well as mixes of these different threats.

Furthermore, these controls are not limited to blocking only the initial compromise of systems, but also address detecting already-compromised machines, and preventing or disrupting attacker's actions. The defenses identified through these controls deal with decreasing the initial attack surface through improving architectures and hardening security, identifying already-compromised machines to address long-term threats inside an organization's network, controlling so-called 'superuser' privileges on systems, and disrupting attackers' command-and-control of implanted malicious code. Figure 1 illustrates the scope of different kinds of attacker activities that these controls are designed to help thwart.

The rings represent the actions computer attackers may take against target machines. These actions include initially compromising a machine to establish a foothold by exploiting one or more vulnerabilities (i.e., "Getting In"). Attackers can then maintain long-term access on a system, often by creating accounts, subverting existing accounts, or altering the software on the machine to include backdoors and rootkits (i.e., "Staying In"). Attackers with access to machines can also cause damage, which could include stealing, altering, or destroying information; impairing the system's functionality to jeopardize its business effectiveness or mission; or using it as a jump-off point for compromise of other systems in the environment (i.e. "Acting"). Where these rings overlap, attackers have even more ability to compromise sensitive information or cause damage. Outside of each set of rings in the figure, various defensive strategies are presented, which are covered throughout the controls described in this document. Defenses in any of the rings helps to limit the abilities of attackers, but improved defenses are required across all three rings and their intersections. It is important to note that the CAG is designed to help improve defenses across each of these rings, rather than on merely preventing initial compromise.
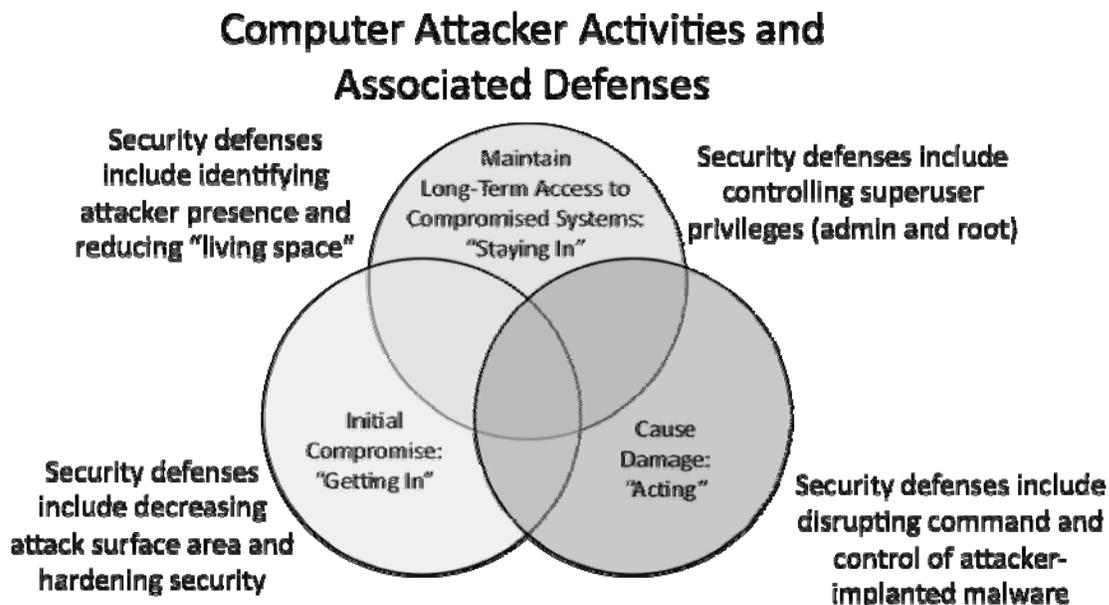


**Figure 1: Types of Computer Attacker Activities these Controls Are Designed to Help Thwart**

**Relationship to Other Federal Guidelines, Recommendations, and Requirements**

These Consensus Audit Guidelines are meant to reinforce and prioritize some of the most important elements of the guidelines, standards, and requirements put forth in other US Government documentation, such as NIST special publication 800-53: *Recommended Security Controls for Federal Information Systems*, SCAP, FDCC, FISMA, and Department of Homeland Security Software Assurance documents. These guidelines do not conflict with such recommendations. In fact, the guidelines set forth herein are a proper subset of the recommendations of 800-53, designed so that organizations can focus on a specific set of actions associated with current threats and computer attacks they face every day. A draft of the mapping of individual guidelines in this document to specific recommendations of 800-53 is included in Appendix A.

Additionally, the Consensus Audit Guidelines are not intended to be comprehensive in addressing everything that a CIO or CISO must address in an effective security program. For example, in addition to implementing controls identified in this document, organizations must develop appropriate security policies, security architectures, and system security approvals. Furthermore, CIOs and CISOs must balance business needs and security risks, recognizing that there are sometimes trade-offs between them that must be carefully analyzed and measured.

**Periodic and Continual Testing of Controls**

Each control included in this document describes a series of tests that organizations can conduct on a periodic or, in some cases, continual basis to ensure that appropriate defenses are in place. One of the goals of the tests described in this document is to provide as much automation of testing as possible. By leveraging standardization efforts and repositories of content like SCAP, these automated test suites and scripts can be highly sharable between organizations, consistent to a large extent, and easily used by auditors for validation. However, at various phases of the tests, human testers are needed to set up tests or evaluate results in a fashion that cannot be automated. The testers associated with measuring such controls must be trusted individuals, as the test may require them to access sensitive systems or data in the course of their tests. Without appropriate authorization, background checks, and possibly clearance, such tests may be impossible. Such tests should also be supervised or reviewed by appropriate agency officials well versed in the parameters of lawful monitoring and analysis of information technology systems.

**A Work in Progress**

The consensus effort to define critical security controls is a work in progress. In fact, changing technology and changing attack patterns will necessitate future changes even after it has been adopted. In a sense, this will be a living document moving forward, but the controls described in this version are a solid start on the quest to make fundamental computer security hygiene a

well-understood, repeatable, measurable, scalable, and reliable process throughout the federal government.

# DESCRIPTION OF CONTROLS

## Critical Control 1: Inventory of authorized and unauthorized hardware.

**How do attackers exploit the lack of this control?**

Many criminal groups and nation states deploy systems that continuously scan address spaces of target organizations waiting for new, unprotected systems to be attached to the network. The attackers also look for laptops not up to date with patches because they are not frequently connected to the network. One common attack takes advantage of new hardware that is installed on the network one evening and not configured and patched with appropriate security updates (i.e., "hardened") until the following day. Attackers from anywhere in the world may quickly find and exploit such systems that are Internet-accessible. Furthermore, even for internal network systems, attackers who have already gained internal access may hunt for and compromise additional improperly secured internal computer systems. The attackers use the night-time window to install backdoors on the systems that are still present after the systems are hardened and are used for exfiltration of sensitive data from compromised systems and from other systems connected to it.

Additionally, attackers frequently look for experimental or test systems that are briefly connected to the network but not included in the standard asset inventory of an organization. Such experimental systems tend not to have as thorough security hardening or defensive measures as other systems on the network. Although these test systems do not typically hold sensitive data, they offer an attacker an avenue into the organization, and a launching point for deeper penetration.

**How can this control be implemented, automated, and its effectiveness measured?**

An accurate and up-to-date inventory, controlled by active monitoring and configuration management can reduce the chance of attackers finding unauthorized (those not previously approved for installation) and unprotected systems to exploit.

1. Vis/Attrib: Maintain an asset inventory of all computer systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, and an asset owner responsible for each device.
2. Vis/Attrib: Ensure that network inventory monitoring tools are operational and continuously monitoring, keeping the asset inventory up to date and looking for deviations from the expected inventory of assets on the network, and alerting the security operations center when deviations are discovered.

3. Config/Hygiene: Secure the asset inventory database and related systems, ensuring that they are included in periodic vulnerability scans and that asset information is encrypted.
4. Config/Hygiene: Implement automated configuration management control mechanisms for tracking and approving changes made to systems.  These controls should address both hardware and software changes, network configuration changes, and any other modifications affecting security of the system.
5. Config/Hygiene: Periodically attach several hardened computer systems not already included in asset inventories to the network and measure the delay before each device connection is disabled or the installers confronted.
6. Advanced: In addition to an inventory of hardware, organizations should develop an inventory of information assets, which identifies their critical information and maps critical information to the hardware assets on which it is located.

**Procedures and tools for implementing and automating this control:**

Some organizations maintain asset inventories using specific large-scale enterprise commercial products dedicated to the task or they use free solutions to track and then sweep the network periodically for new assets connected to the network.  In particular, when effective organizations acquire new systems, they record the owner and asset features of each system, including its network interface MAC address, a unique identifier hard-coded into each network interface, including Ethernet and wireless interfaces.  This mapping of asset attributes and owner to MAC address can be stored in a free or commercial database management system.

Then, with the asset inventory assembled, many organizations use tools to pull information from network assets such as switches and routers regarding the machines connected to the network.  Using the Cisco Discovery Protocol (CDP), the Simple Network Management Protocol (SNMP), and other vehicles, software retrieves MAC addresses and other information that can be reconciled with the organization's asset inventory.

Going further, effective organizations configure free or commercial network scanning tools to perform network sweeps on a regular basis, such as every 12 hours, sending a variety of different packet types to identify devices connected to the network.  At a minimum, the network scan sends traditional ping packets (ICMP Echo Request), looking for ping responses to identify a system at a given IP address.  In addition to traditional pings, scanners can also identify devices on the network using TCP SYN or ACK packets.  Once they have identified IP addresses of devices on the network, the better scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.  Unfortunately, unless the scanner is on the same subnet of a discovered target machine, or has administrative credentials to login to the discovered asset, it is unable to pull the MAC address of the discovered network interface.  Still, the IP address and operating system information can be reconciled against the organization's asset inventory assembled in the asset database and regularly updated.

Wireless devices (and wired laptops) may periodically join a network and then disappear making the inventory of currently available systems churn significantly. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused, because they are merely files in some host machine's file system. Additionally, remote machines accessing the network using VPN technology may appear on the network for a time, and then be disconnected from it. Each machine, whether physical or virtual, directly connected to the network or attached via VPN, currently running or shut down, should be included in an organization's asset inventory.

To evaluate the effectiveness of the asset inventory and its monitoring, an organization should connect a fully patched and hardened machine to the network on a regular basis, such as monthly, to determine whether that asset appears as a new item in the network scan, the automated inventory, and/or asset management database.

Sandia National Labs takes the inventory a step further by requiring the name and contact information of a system administrator responsible for each element in its inventory. Such information provides near instantaneous access to the people in a position to take action when a system at a given IP address is found to have been compromised.

## Critical Control 2: Inventory of authorized and unauthorized software; enforcement of white lists of authorized software.

### How do attackers exploit the lack of this control?

Computer attackers deploy systems that continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited. Sophisticated attackers may use "zero-day" exploits – which take advantage of vulnerabilities for which no patch has yet been released by the software vendor. Those that do not enforce white lists of authorized applications make their systems more vulnerable. Such machines are more likely to be running software that is unneeded for business purposes, introducing security flaws. Furthermore, machines without white lists of authorized applications provide an easier target for attackers to exploit to run their own unauthorized software. Once a single machine is exploited, the attackers use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. One compromised machine can turn into many. Organizations that do not have complete software inventories are unable to find systems running software likely to have been compromised by exploits, because they do not know which systems are running what software.

**How can this control be implemented, automated, and its effectiveness measured?**

1. Vis/Attrib: Deploy software inventory tools throughout the organization covering each of the operating system types in use, including desktop, server, and network devices. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level. The tool should also monitor for unauthorized software.
2. Vis/Attrib: Ensure software inventory monitoring tools are operational by periodically installing several software updates and new packages on hardened control machines in the network and measure the delay before the software inventory indicates the changes. Such updates should be chosen for the control machines so that they do not negatively impact production systems on the network. Also measure the organization's response activities to unauthorized software installed in the environment.
3. Config/Hygiene: A policy is also required to force all drivers to be digitally signed and the organization should configure systems to block the loading of drivers that are not signed by a trusted software vendor. Both Windows Vista and Windows XP include configuration options that can enforce driver signing across an organization. Strictly loading only signed drivers is a crucial step toward blocking intruders' control of systems via rootkits that modify the core of the operating system to wield control.

**Procedures and tools for implementing and automating this control:**
Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provide an inventory check of hundreds of common applications used in enterprises on Microsoft Windows and other machines, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging the standardized application names in CPE.

Features that implement white and black lists of programs allowed to run or blocked from executing are included in modern end-point security suites. Moreover, commercial solutions are increasingly bundling together anti-virus, anti-spyware, personal firewall, and host-based Intrusion Detection Systems and Intrusion Prevention Systems (IDS and IPS). In particular, most endpoint security solutions can look at the name, file system location, and/or MD5 hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom whitelists and blacklists based on executable path, hash, or regular expression matching. Some even include a graylist function that allows administrators to define rules for execution of specific programs only by certain users and at certain times of day and blacklists based on specific signatures.

Once software inventory and execution control products are deployed, they can be evaluated by attempting to run a black listed program or a program that is not on the whitelist. To test solutions that implement a black list, the organization can define a specific benign executable

as not being allowed, such as a simple word processor contained in a single EXE file. They can then attempt to run the program and test whether execution is blocked, and whether an alert is generated. For white-list solutions, the organization can attempt to run a similar benign executable not on the white-list, again checking for blocked execution and alerts.

## Critical Control 3: Secure configurations for hardware and software on laptops, workstations, and servers.

**How do attackers exploit the lack of this control?**

On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way that it was delivered from manufacturers and resellers, thereby being immediately vulnerable to exploitation. Attackers attempt to exploit both network-accessible services and browsing client software using such techniques. The two possible defenses against these automated exploits are to ask every computer user to reconfigure systems to be more securely configured or to buy and install computer and network components with the secure configurations already implemented and to update these configurations on a regular basis. Despite a majority of agencies that still use the former approach, only the latter approach (i.e., updating configurations on a regular basis) is effective. Establishing and monitoring secure configurations provide the motivation to the agency to ensure systems are purchased with secure configurations baked in.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: System images must have documented security settings, be approved by an agency change control board, and registered with a central image library for the agency or multiple agencies. Government agencies should negotiate contracts to buy systems configured securely out of the box using these images, which should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities. These images should be validated and refreshed on a regular basis (such as every six months) to update their security configuration in light of recent vulnerabilities and attack vectors. The master images themselves must be stored on securely configured servers, with integrity checking tools and change management to ensure only authorized changes to the images are possible.
2. QW: Change factory default settings on hardware and software and implementing network hardening procedures. This would typically include removal of unnecessary usernames and logins, as well as the disabling or removal of unnecessary services. Such hardening also involves, among other measures, applying patches, closing open and

unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and firewalls.

3. QW: At least once per month, run assessment programs on a varying random sample of systems to measure the number that are and are not configured according to the secure configuration guidelines.  Provide senior executives with charts showing the number of systems that match configuration guidelines versus those that do not match, illustrating the change of such numbers month by month for each organizational unit.

4. Vis/Attrib: Implement and test a vulnerability monitoring system to ensure it measures all secure configuration elements that can be measured through remote testing, using features such as those included with SCAP to gather configuration vulnerability information. Provide senior executives with charts showing the number of vulnerabilities identified, separated out for comparison based on organizational units.

**Procedures and tools for implementing this control:**

Organizations can implement this control using commercial and/or free vulnerability scanning tools that evaluate the security configuration of machines and software.  Some have also found commercial services using remotely managed scanning appliances to be effective as well.  To help standardize the definitions of discovered vulnerabilities in multiple departments of an agency or even across agencies, it is preferred to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF.  In addition, recent changes in licensing associated with popular free vulnerability scanners require users to pay for certain modules, blurring the line between free and commercial tools.

Advanced vulnerability scanning tools can be configured with user credentials to login to scanned systems and perform more comprehensive scans than can be achieved without login credentials.  For example, organizations can run scanners every week or every month without credentials for an initial inventory of potential vulnerabilities.  Then, on a quarterly or semi-annual basis, the organization can run the same scanning tool with user credentials or a different scanning tool that supports scanning with user credentials to find additional vulnerabilities.

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed.  Such tools can provide fine-grained insight into unauthorized changes in configuration or the introduction of security weaknesses inadvertently by administrators.

Effective organizations link their vulnerability scanners with problem ticketing systems that automatically monitor and report progress on fixing problems and that make visible

unmitigated critical vulnerabilities to higher levels of management to ensure the problems are solved.


## Critical Control 4: Secure configurations of network devices such as firewalls, routers, and switches.

**How do attackers exploit the lack of this control?**

Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, the exceptions are deployed, and those exceptions are not undone when the business need is no longer applicable.  Making matters worse, in some cases, the security risk of the exception is never properly analyzed, nor is this risk measured against the associated business need.  Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses.   Attackers have exploited flaws in these network devices to redirect traffic on a network (to a malicious system masquerading as a trusted system), and to intercept and alter information while in transmission.  Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization.   The security configuration of such devices should be documented, reviewed, and approved by an agency change control board.
2. QW: At network interconnection points, such as Internet gateways, inter-agency connections, and internal network segments with different security controls, implement ingress and egress filtering to allow only those ports and protocols with a documented business need, monitor traffic flows looking for attacks using intrusion detection technology, and log each connection for a period of at least 30 days.
3. QW: Network devices that filter unneeded services or block attacks (including firewalls, network-based Intrusion Prevention Systems, routers with access control lists, etc.) should be tested under laboratory conditions with each given organization's configuration to ensure that these devices fail in a closed/blocking fashion under significant loads with traffic including a mixture of legitimate allowed traffic for that configuration intermixed with attacks at line speeds.
4. Config/Hygiene: All new configuration rules beyond a baseline hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPSs, should be documented with a specific business reason for the

change, a specific individual's name responsible for that business need, and an expected duration of the need.  At least once per quarter, these rules should be reviewed to determine whether they are still required from a business perspective.  Expired rules should be removed.

5. Config/Hygiene: Periodically attempt to penetrate network devices by simulating attacker's actions against such devices.  Such testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an agency) as well from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

6. Config/Hygiene: Network infrastructure devices should be managed using two-factor authentication and encrypted sessions.

7. Advanced: The network infrastructure should be managed across network connections that are separated from the business use of that network, relying on separate VLANs or preferably relying on entirely different physical connectivity for management sessions for network devices.

**Procedures and tools for implementing this control:**

Port scanners and most vulnerability scanning tools can be used to attempt to launch packets through the device, measuring all TCP and UDP ports. This measures the effectiveness of the firewall's configuration.  A sniffer can be set up on the other side of the firewall to determine which packets are allowed through the device.  The results of the test can be matched against the list of services that are allowed both inbound and outbound (defined through policy that should represent documented business needs for each allowed service), thereby identifying misconfigured firewalls.  Such measurement should be conducted at least every quarter, and also when significant changes are made to firewall rule sets and router access control lists.

More effective organizations use commercial tools that evaluate the rule set of firewalls and routers with access control lists to determine whether they are consistent or in conflict, providing an automated sanity check of network filters and search for errors in rule sets or ACLs that may allow unintended services through the device.  Such tools should be run each time significant changes are made to firewall rule sets or router access control lists.

# Critical Control 5: Boundary Defense

**How do attackers exploit the lack of this control?**

Attackers target Internet-facing systems because they are accessible. They use weaknesses they find there as jumping off points to get inside the boundary to steal or change information or to

set up persistent presence for later attacks.  Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

Boundary defenses to stop these types of attack have multiple dimensions: all Internet and extranet traffic passes through managed, authenticated proxies, a DMZ is employed that is separated from internal systems either physically or through tightly monitored filtering, and securely configured firewalls and intrusion detection systems are deployed at each gateway.

**How can this control be implemented, automated, and its effectiveness measured?**

The boundary defenses included in this control build on the network element hardening described in Critical Control 4 above, with these additional recommendations focused on improving the overall architecture and implementation of both Internet and internal network boundary points.  Internal network segmentation is central to this control because once inside a network, intruders target the most sensitive machines.  Usually, internal network protections are not set up to defend against an internal attacker.  Setting up even a basic level of security segmentation across the network and protecting each segment with a proxy and a firewall will greatly reduce the intruders' access to the other parts of the network.

Enhance network access controls in conjunction with authentication controls to deter propagation through the network from business unit to business unit.  Add layers of network protection to critical services on the network, creating a layered access path using application authentication and network segmentation. Implement internal ACL's, internal proxies and firewalls to limit access to these areas. This will deter the intruders from gaining unauthorized access to these areas and could limit their activity altogether.

1. QW: Deploy IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems.  These sensors should be configured to record at least packet header information, and preferably full packet header and payloads of the traffic passing through the network border.
2. Vis/Attrib: Define a network architecture that clearly separates internal systems from DMZ systems and extranet systems.  DMZ systems are machines that need to communicate with the internal network as well as the Internet, while extranet systems are systems whose primary communication is with other systems at a business partner.
3. Vis/Attrib: Design and implement network perimeters so that all outgoing web, ftp, and ssh traffic to the Internet must pass through at least one proxy on a DMZ network.  The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses; and being able to be configured with white lists of allowed sites to be accessed through the proxy.
4. Vis/Attrib: Require all remote access (including VPN, dial-up, and other forms) to use two-factor authentication.

5. Config/Hygiene: Conduct periodic penetration tests against DMZs from the Internet to determine whether the attacks are detected and/or thwarted.
6. Config/Hygiene: Periodically scan for back-channel connections to the Internet that bypass the DMZ.
7. Config/Hygiene: To limit access by an insider or malware spreading on an internal network, organizations should devise internal network segmentation schemes to limit traffic to only those services needed for business use across the internal network.
8. Config/Hygiene: Organizations should develop plans for rapidly deploying filters on internal networks to help stop the spread of malware or an intruder.
9. Advanced: Force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Most organizations already use domain authentication to traverse these routes, and could implement additional authentication through external proxy servers that require a daily password.
10. Advanced: To help identify covert channels exfiltrating data through a firewall, built-in firewall session tracking mechanisms included in many commercial firewalls should be configured to identify long-term TCP sessions that last over one hour, alerting personnel about the source and destination addresses associated with these long-term sessions.
11. Advanced: Require all authentication, both internal and external, to use two-factor authentication.

**Procedures and tools for implementing this control:**

One element of this control can be implemented using free or commercial intrusion detection systems (IDSs) and sniffers to look for attacks from external sources directed at DMZ and internal systems, as well as attacks originating from internal systems against the DMZ or Internet.  Security personnel should regularly test these sensors by launching vulnerability-scanning tools against them to verify that the scanner traffic triggers an appropriate alert.   The captured packets of the IDS sensors should be reviewed using an automated script each day to ensure that log volumes are within expected parameters and that the logs are formatted properly and have not been corrupted.

Additionally, packet sniffers should be deployed on DMZs to look for HTTP traffic that bypasses HTTP proxies.  By sampling traffic regularly, such as over a 3-hour period once per week, information security personnel search for HTTP traffic that is neither sourced by or destined for a DMZ proxy, implying that the requirement for proxy use is being bypassed.

To identify back-channel connections that bypass approved DMZs, effective network security personnel establish an Internet-accessible system to use as a receiver for testing outbound access.   This system is configured with a free or commercial packet sniffer.  Then, security personnel connect a sending test system to various points on the organization's internal network, sending easily identifiable traffic to the sniffing receiver on the Internet.  These packets can be generated using free or commercial tools with a payload that contains a custom

file used for the test.  When the packets arrive at the receiver system, the source address of the packets should be verified against acceptable DMZ addresses allowed for the organization.  If source addresses are discovered that are not included in legitimate, registered DMZs, more detail can be gathered by using a traceroute tool to determine the path packets take from the sender to the receiver system.

# Critical Control 6: Maintenance, Monitoring and Analysis of Complete Audit Logs
**How do attackers exploit the lack of this control?**

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines.  Even if the victims know that their systems were compromised, without protected and complete logging records, the victim is blind to the details of the attack and to the subsequent actions taken by the attackers after they gained the initial foothold.  Sometimes logging records are the only evidence of a successful attack.  Many organizations keep audit records for compliance purposes but attackers rely on the fact that such organizations rarely look at the audit logs so they do not know that their systems have been compromised.   Because of poor or non-existent log analysis techniques, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include dates, timestamps, source addresses, destination addresses, and various other useful elements of each packet and/or transaction.  Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression (CEE).  If systems cannot generate logs in a standardized format, deploy log normalization tools to convert logs into a standardized format.
2. QW: Ensure that all systems which store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals.
3. QW: System administrators and security personnel should devise profiles of common events from given systems, so that they can tune detection of attacks by avoiding false positives, more rapidly identify anomalies, and avoid overwhelming analysts with alerts.
4. QW: All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely.

5. QW: Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions.
6. QW: Verify that security administrators run bi-weekly anomaly reports and actively review the anomalies.
7. Vis/Attrib: Each agency network should include synchronized time sources, from which all servers retrieve time information on a regular basis, so that timestamps in logs are consistent.
8. Vis/Attrib: Network boundary devices, including firewalls, network-based IPSs, and both inbound and outbound proxies should be configured to log verbosely all traffic (both allowed and blocked) arriving at the device.
9. Vis/Attrib: DNS servers should be configured to log all DNS requests and responses, provided that capturing such logging detail is reasonable for the given DNS server's load.
10. Vis/Attrib: Ensure logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.
11. Vis/Attrib: Deploy a Security Event/Information Management (SEIM) system tool for log aggregation and consolidation from multiple machines and for log correlation and analysis. Deploy and monitor standard government scripts for analysis of the logs, as well as using customized local scripts. Furthermore, event logs should be correlated with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. And, secondly, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a known-vulnerable target.
12. Vis/Attrib: Ensure analytical programs that review audit logs are run at least once per day.
13. Config/Hygiene: Periodically test the audit analysis process by inserting audit test records that demonstrate system compromise and measure the amount of time that passes before the compromise is discovered and action is taken.
14. Config/Hygiene: Periodically test the audit logging records to ensure they have the content needed using standard audit content lists for systems on each level of criticality.

**Procedures and tools for implementing this control:**

Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging should a follow-up investigation be required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset

inventory assembled as part of Critical Control 1, to ensure that each managed item that is actively connected to the network is periodically generating logs.

"Analytical programs" for reviewing logs can be useful, but the capabilities employed to analyze audit logs is quite wide-ranging, including just a cursory examination by a human. Actual correlation tools can make the logs far more useful for subsequent manual inspection by people. The measurements above do not require correlation tools be deployed, given their cost and complexity, but such tools can be quite helpful in identifying subtle attacks. Such tools are not a panacea, however, and are not a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are required to identify and understand attacks.

## Critical Control 7: Application Software Security

**How do attackers exploit the lack of this control?**

Attacks against vulnerabilities in applications have been a top priority for criminal organizations since 2005. In that year the attackers focused on exploiting vulnerabilities in ubiquitous products such as anti-virus tools and back-up systems. These attacks continue – with new vulnerabilities in security products and in back-up tools being discovered and exploited each week. A second, massive wave of application attacks began surging in late 2006 when the criminals went after custom-developed web, server, and workstation applications. They found fertile territory. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites. Trusted organizations in state governments, the United Nations, and similarly respected organizations infected hundreds or thousands of PCs, turning them into zombies. Many more web and non-web application attacks are emerging. On average more than 70 new vulnerabilities are found every week in commercial applications – and many more are waiting to be found (or have already been exploited without public recognition) in custom applications written by programmers for individual sites in government, commercial, and private enterprises.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Test web and other application code for source code errors prior to deployment using automated source code analysis software, if source code is available. In particular, input validation and output encoding routines of application software should be carefully reviewed and tested.
2. QW: Test web applications for common security weaknesses using web application scanners prior to deployment and then no less often than weekly as well as whenever updates are made to the application.

3. Config/Hygiene: Verify that security is embedded in the application development life cycle of all applications.
4. Config/Hygiene: Protect web applications by deploying web application firewalls that inspect all traffic flowing to the web application for common web application attacks, including but not limited to Cross-Site Scripting, SQL injection, command injection, and directory traversal attacks.  For applications that are not web based, deploy specific application firewalls if such tools are available for the given application type.

**Procedures and tools for implementing this control:**

Source code testing tools, web application security scanning tools, and object code testing tools have proven useful in securing application software, along with manual application security penetration testing by testers who have extensive programming knowledge as well as application penetration testing expertise.  The Common Weakness Enumeration (CWE) is utilized by many such tools to identify the weaknesses that they find.  Organizations can also use CWE to determine which types of weaknesses they are most interested in addressing and removing.  A broad community effort to identify the "Top 25 Most Dangerous Programming Errors" is available as a minimum set of important issues to investigate and address.  When evaluating the effectiveness of testing for these weaknesses, the Common Attack Pattern Enumeration and Classification (CAPEC) can be used to organize and record the breadth of the testing for the CWEs as well as a way for testers to think like attackers in their development of test cases.

# Critical Control 8: Controlled Use of Administrative Privileges

**How do attackers exploit the lack of this control?**

Two very common attacker techniques take advantage of uncontrolled administrative privileges.  In the first, a workstation user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious web site, or simply surfing to a website hosting attacker content that can automatically exploit browsers.  The file or exploit contains executable code that runs on the victim's machine. If the victim's computer is running with administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data.  The second common technique used by attackers is elevation of privileges after using a vulnerable service or a guessed password to gain access to a server.  If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of the servers, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.  One of the most common of these attacks involves the domain administration privileges in large Windows environments,

giving the attacker significant control over large numbers of machines and access to the data they contain.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Inventory all administrative passwords and validate (through automation) that each person with administrative privileges is authorized by a senior executive and that his/her administrative password has at least 12 semi-random characters, consistent with the Federal Desktop Core Configuration (FDCC) standard. In testing this control, also ensure that no administrator username/passwords (domain or local) are reused among systems and applications. In addition to the 12-or-more character password, all administrative access should utilize two-factor authentication.
2. QW: Passwords for all systems should be stored in a hashed or encrypted format. Furthermore, files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with superuser privileges.
3. QW: Ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.
4. QW: Audit passwords to ensure previously used passwords are not being authorized for re-use within a certain time frame (e.g., 6 months).
5. Vis/Attrib: Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior (e.g., system reconfigurations during night shift)
6. Config/Hygiene: Remote access directly to a machine should be blocked for administrator-level accounts. Instead, administrators should be required to access a system remotely using a fully logged and non-administrative account. Then, once logged in to the machine without admin privileges, the administrator should then transition to administrative privileges using tools such as sudo on Linux/UNIX, runas on Windows, and other similar facilities for other types of systems.
7. Config/Hygiene: Conduct targeted spear-phishing attacks against both administrative personnel and non-administrative users to measure the quality of their defense against social engineering and to test whether they are using administrator privileges while reading e-mail or surfing the Internet.
8. Config/Hygiene: Ensure all domain administrator accounts are accessible only with two-factor authentication.
9. Advanced: Segregate admin accounts based on roles (in policy). For example, "Workstation admin" accounts are the only admin accounts capable of logging into workstations, laptops, etc. Domain admin accounts are not allowed to log into workstations and are only allowed to log into servers. The benefit here is that the domain admin accounts (what the bad guys want) will not get cached on the workstations. Makes privilege to domain admin much harder.

**Procedures and tools for implementing this control:**

Built-in operating system features can extract lists of accounts with superuser privileges, such as those in the administrators group on Windows machines and those with UID or GID 0 on Linux and Unix systems.  In Active Directory environments, personnel can use Microsoft Group Policy to dump lists of such users from machines and domain controllers so that these accounts can be reconciled against an inventory of users with legitimate and approved needs for such access.

To verify that users with such high-privileged accounts do not use such accounts for day-to-day web surfing and e-mail reading, security personnel periodically (often sampling weekly) can gather a list of running processes in an attempt to determine whether any browsers or e-mail readers are running with high privileges.  Such information gathering is often scripted, with short shell scripts running the ps command on Linux or the tasklist command on Windows, and analyzing its output for a dozen or more different browsers, e-mail readers, and document editing programs.  Some legitimate system administration activity may require the execution of such programs over the short term, but long-term or frequent use of such programs with administrative privileges could indicate that an administrator is not adhering to this control.

To enforce the requirement for password length (12 characters), built-in operating system features for minimum password length in Windows and Linux can be configured, which prevent users from choosing short passwords.   To enforce password complexity (requiring passwords to be a string of pseudo-random characters), built-in Windows Group Policy configuration settings and Linux Pluggable Authentication Modules (PAM) can be employed.

Log analysis tools are used to look for logs indicating changes to system configuration that are not reconcilable with change management systems to identify alterations potentially made by an intruder.

# Critical Control 9: Controlled Access Based On Need to Know

**How do attackers exploit the lack of this control?**

Once an attacker has penetrated a sensitive network, if users have access to all or most of the information, the attacker's job of finding and exfiltrating important information is greatly facilitated.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Establish a multi-level data identification/separation scheme (such as a three-level system with data separated into categories such as public, all authorized employees, and only a small subset of employees).
2. QW: Very sensitive data, such as passwords and router, switch, and firewall configurations and rulesets, should be encrypted or stored offline
3. Vis/Attrib: Enforce detailed audit logging for access to non-public data and special authentication for sensitive data to frustrate attackers who have penetrated important sites.
4. Config/Hygiene: Periodically, create a standard user account on file servers and other application servers in the organization.  Then, while logged into that test account, have authorized personnel determine whether they can access files owned by other users on the system, as well as critical operating system and application software on the machine.

**Procedures and tools for implementing this control:**

This control is often tested using built-in operating system administrative features, with security personnel scheduling a periodic test on a regular basis, such as monthly.  For the test, the security team creates at least two non-superuser accounts on a sample of server and workstation systems.  With the first test account, the security personnel create a directory and a file that should be viewable only by that account.  They then login to each machine using the second test account to see whether they are denied access to the files owned by the first account.  Similar but more complex test procedures could be devised to verify that accounts with different levels of access to sensitive data are in fact restricted to accessing only the data at the proper classification/sensitivity level.

# Critical Control 10: Continuous Vulnerability Testing and Remediation

**How do attackers exploit the lack of this control?**

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest.  Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Verify that vulnerability testing of networks, systems, and applications are run no less than weekly.  Where feasable, vulnerability testing should occur on a daily basis.
2. Config/Hygiene: Ensure vulnerability testing is performed in authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly, either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested, to overcome limitations of unauthenticated vulnerability testing.
3. Config/Hygiene: Compare the results from back-to-back vulnerability tests to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk.  Such acceptance of business risks for existing vulnerabilities should be periodically reviewed as well, to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.
4. Config/Hygiene: Chart the numbers of unmitigated, critical vulnerabilities, for each department/division and share the reports with senior management to provide effective incentives for mitigation.
5. Config/Hygiene: Measure the delay in patching new vulnerabilities and ensure the delay is equal to or less than the benchmarks set forth by the organization, which should be no more than a week for critical patches unless a mitigating control that blocks exploitation is available.
6. Advanced: Deploy automated patch management tools for all systems for which such tools are available and safe.

**Procedures and tools for implementing this control:**

Organizations can use vulnerability-scanning tools, such as the free and commercial tools described in Critical Control #3.

Effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time.  Security personnel use these features to conduct vulnerability trending from month-to-month.

As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel should determine and document the amount of time that elapsed between the public release of a patch for the system and the occurrence of the vulnerability scan.  If this time window exceeds the organization's benchmarks for deployment of the given patch's criticality level, security personnel should note the delay and determine if a deviation was formally documented for the system and its patch.  If not, the security team should work with management to improve the patching process.

# Critical Control 11: Dormant Account Monitoring and Control

**How do attackers exploit the lack of this control?**

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
2. QW: Monitor account usage to determine dormant accounts that have not been used for a given period, such as thirty days, notifying the user or user's manager of the dormancy. After a longer period, such as sixty days, the account should be disabled.
3. QW: Match active employees and contractors with all accounts and disable accounts that are not assigned to active employees or contractors.
4. Vis/Attrib: Monitor attempts to access deactivated accounts through audit logging.
5. Config/Hygiene: Profile each user's typical account usage by determining normal time-of-day access and access duration for each user. Generate daily reports that indicate users who have logged in during unusual hours or have exceeded their normal login duration by 150%.

**Procedures and tools for implementing this control:**

A test account should be created every month, with very limited privileges so that it cannot access anything except public files on a system. No user should log into this test account. Any login activity to this test account should be investigated immediately. Automated software should check to ensure that the system generates a notice about such a test account after thirty days of non-use. Furthermore, an automated script should verify that the account has been disabled sixty days after the account was first created, notifying security personnel if the account has not been automatically disabled. At the end of this test interval, the first test account should be deleted, with a new limited test account created for the next round of automated checking.

# Critical Control 12: Anti-Malware Defenses

**How do attackers exploit the lack of this control?**

Tens of thousands of viruses and other malicious code examples are circulating on the Internet either in email attachments or downloaded from web sites or through other means of delivery. Some malicious code actually turns anti-malware features off, giving the attacker's malware unfettered access to the system.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Monitor workstations, servers, and mobile devices for active, up to date anti-malware protection with anti-virus, anti-spyware, and host-based Intrusion Prevention System functionality. Enterprise administrative features should be used to check daily the number of systems that do not have the latest anti-malware signatures, keeping the number of such systems small or eliminating them entirely through rapid and continuous updates. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.
2. QW: Employ software auto update features and or have administrators manually push updates to all machines on a regular basis. After applying an update, set up systems to automatically verify the update status of a machine.
3. QW: Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, or CDs/DVDs.
4. QW: Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.
5. Config/Hygiene: New updates to the malware signature base of each anti-malware tool should be tested in a non-production environment to verify that it does not negatively impact systems before it is pushed to production machines.
6. Config/Hygiene: To verify that anti-malware solutions are running, periodically introduce a benign, non-spreading test case, such as the EICAR anti-virus test file, onto a system in the environment to ensure that it is detected by the anti-malware system, and that the detection is reported to the enterprise management system.
7. Advanced: Deploy honeypots or tarpits as detection mechanisms that can also slow down an attacker's progress inside a network.

**Procedures and tools for implementing this control:**

Relying on policy and user action to keep anti-malware tools up to date has been widely discredited; it doesn't work. To ensure anti-virus signatures are up to date, effective organizations use automation. They use the built-in administrative features of enterprise end-

point security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results, to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.  For added security in depth, and for those systems that may fall outside the enterprise anti-malware coverage, they use network access control technology that tests machines for compliance with security policy before allowing them to connect to the network.

On a regular basis, such as monthly, effective organizations download and test the free EICAR file to verify that anti-virus protection is functioning on a sampling of protected workstations and servers.  Anti-malware tools should detect this benign file, and security personnel verify that the detection event is noted in enterprise monitoring and alerting systems.

Organizations can use commercial software update products on Windows and various free Linux software update tools to deploy patches and up-to-date versions of software throughout an environment.  To verify that such software is successfully deployed, the update tool itself is run to check the version installed on a sample of enterprise systems.  Other organizations use a commercial version-checking tool to ensure that updates have been applied to systems.

Advanced: Some enterprises deploy the free honeypot and tarpit tools to identify attackers in their environment, running this free software running on low-cost hardware.  Security personnel continuously monitor honeypots and tarpits to determine whether traffic is directed to them and account logins are attempted.  When they identify such events, these personnel gather the source address from which this traffic originates for a follow-on investigation.

# Critical Control 13: Limitation and Control of Ports, Protocols and Services

**How do attackers exploit the lack of this control?**

Attackers search for services that have been turned on and that can be exploited. Common examples are web servers, mail servers, file and print services, and DNS servers. Many software packages automatically install services and turn them on as part of the installation of the main software package without ever informing the user that the services have been enabled. Because the user does not know about the services, it is highly unlikely that that the user will actively ensure the services are disabled if they are not being used or regularly patched if they are being used.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Network perimeters should implement both ingress and egress filtering, allowing only those services and protocols that have a defined, documented business need for the organization. A 'default to deny' rule should be applied between firewalled networks, with only specific services allowed through.
2. Config/Hygiene: Host-based firewalls or port filtering tools should be applied on end systems, again with a default deny rule.
3. Config/Hygiene: Configuration and vulnerability testing tools should be tuned to compare services that are listening on each machine against a list of authorized services. The tools should be further tuned to identify changes over time on systems for both authorized and unauthorized services. Use government-approved scanning files to ensure minimum standards are met.
4. Config/Hygiene: Implement hardening recommendations from guidelines for underlying operating systems and installed applications, such as those found in mandatory STIG (Secure Technical Implementation Guides) requirements, NIST configuration guidelines, or Center for Internet Security hardening guides, if they exist for the given technology.
5. Config/Hygiene: Periodically, a secure version of an authorized service should be activated on a relatively unimportant system to verify that the change is flagged by the configuration and vulnerability testing tools in the environment.

**Procedures and tools for implementing this control:**
Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation, in an asset management system, such as those described in Critical Control #1. Recently added features in these port scanners are being used to determining the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

To evaluate their scanning procedures, information security personnel often run a free network listening tools on a sample machine, configured simply to listen on a given TCP port associated with a common service, such as Secure Shell (TCP 22), HTTP (TCP 80), or SMB (TCP 445). Such tools are configured merely to listen and then respond when they see a connection request, without providing any useful function or service on the sampled machine, minimizing the exposure to this machine during the test. With this benign listener in place, the automated scanning functionality can be verified to ensure that it discovers the change with the new port listening in the environment.


# Critical Control 14: Wireless Device Control

**How do attackers exploit the lack of this control?**

One of the largest data thefts in history was initiated by an attacker sitting in a car in a parking lot and breaking through the organization's security perimeter by connecting wirelessly to an access point inside the organization. Other wireless devices accompanying travelling officials are being infected every day through remote exploitation during air travel or in a cyber café. Such exploited systems are then being used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points discovered on their network, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient attack vector.

**How can this control be implemented, automated, and its effectiveness measured?**

1. QW: Ensure that each wireless device that is connected to the network matches an authorized configuration and security profile. Deny access to those wireless devices that do not.
2. QW: Ensure that all wireless access points are manageable using enterprise management tools. Access points designed for home use often lack such enterprise management capabilities, and should therefore not be used.
3. Vis/Attrib: Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise. In addition to WIDS, all wireless traffic should be monitored by a wireline IDS as traffic passes into the wireline network.
4. Config/Hygiene: Configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (BIOS or EFI), with password protections to lower the possibility that the user will override such configurations.
5. Config/Hygiene: Regularly scan for unauthorized or misconfigured wireless infrastructure devices, using techniques such as "war driving" to identify access points and clients accepting peer-to-peer connections. Such unauthorized or misconfigured devices should be removed from the network, or have their configurations altered so that they comply with the security requirements of the organization.
6. Config/Hygiene: Ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection.
7. Config/Hygiene: Ensure wireless networks use authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.
8. Config/Hygiene: Ensure wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.
9. Config/Hygiene: Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.

10. Config/Hygiene: Disable Bluetooth wireless access of devices, unless such access is required for a documented business need.
11. Advanced: Configure all wireless clients used to access agency networks or handle organization data in a manner so that they cannot be used to connect to public wireless networks or any other networks beyond those specifically allowed by the agency.

**Procedures and tools for implementing this control:**

Effective organizations run commercials wireless scanning, detection, and discovery tools as well as commercial wireless intrusions detection systems. To evaluate the effectiveness of such tools, security personnel could periodically activate an isolated wireless access point, which has no physical or wireless connectivity to a production network, from within a building monitored by a WIDS device. The team should determine whether the alerting system is triggered by the test access point, and record the amount of time such detection required.

Additionally, the security team could periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates. When devices that are relying on weak wireless security settings are identified, they should be found within the organization's asset inventory and either reconfigured more securely or denied access to the agency network.

# Critical Control 15: Data Leakage Protection

**How do attackers exploit the lack of this control?**

Attackers have exfiltrated more than 20 terabytes of often sensitive data from Department of Defense and Defense Industrial Base (i.e., contractors doing business with the DoD) organizations. Yet, in most cases, the victims had no clue that huge amounts of sensitive data were leaving their site – because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

**How can this control be implemented, automated, and its effectiveness measured?**
1. QW: Set up and enforce rules and policies regarding the use of social network sites, posting information on the commercial web sites, and sharing account information, all of which could be useful for an attacker.
2. QW: Configure firewalls and proxies to enforce limits of file sizes that can be transferred. Allow large file transfers only after prior registration with security personnel.

3. QW: Deny communications with (or limit data flow to) known malicious IP addresses (black lists) or limit access to trusted sites (white lists). Periodically, test packets from bogon source IP addresses should be sent into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses (unroutable or otherwise unused IP addreses) are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.
4. QW: Develop and implement a "Data Protection Strategy" that defines procedural and technical mechanisms for protecting data at rest, data in use, and data in-transit. Specific computer systems and networks housing sensitive data should be inventoried. To the extent possible, applications and systems should be designed that store data on protected servers, rather than storing it on workstation or laptop machines.
5. Vis/Attrib: Network monitoring tools should analyze outbound traffic looking for a variety of anomalies, including large file transfers, long-time persistent connections, unusual protocols and ports in use, and possibly the presence of certain keywords in the data traversing the network perimeter. More sophisticated analyses of network traffic, such as transfer ratios at the workstation level, should be used once government-wide analysis uncovers effective parameters for such analyses. Furthermore, network monitoring tools must have the ability to do immediate network forensics to confirm the nature of the anomalies and to serve as a tuning mechanism to refine anomaly tools.
6. Config/Hygiene: Data should be moved between networks using secure, authenticated, encrypted mechanisms.
7. Config/Hygiene: Data stored on removable, easily transported storage media, such as USB tokens (i.e., "thumb drives"), USB portable hard drives, and CDs/DVDs, should be encrypted. Systems should be configured so that all data written to such media is automatically encrypted without user intervention.
8. Advanced: Deploy an automated tool on network perimeters that monitors for certain keywords and other document characteristics in an automated fashion to determine attempts to exfiltrate data in an unauthorized fashion across network boundaries and block such transfers while alerting information security personnel.
9. Advanced: Configure systems so that they will not write data to USB tokens or USB hard drives.
10. Advanced: Do not use account login names in user's email addresses.

**Procedures and tools for implementing this control:**
Periodically, such as once per quarter, information security personnel should run a script that purposely tries to trigger the data leak protection functionality deployed at network perimeters by sending innocuous data with characteristics (such as certain key words, file size, or source address) to a test system located just outside the data leakage protection device and the firewall. These personnel should ensure that the attempted transfer was detected and an alert was generated, and should also investigate whether the transfer was successfully blocked.

The following paragraphs identify additional controls that are important but that cannot be automatically or continuously monitored. It should be noted that these controls overlap to a greater degree than the ones in the previous section.

## Critical Control 16: Secure Network Engineering

Many controls in this document are effective but can be circumvented in networks that are badly designed. Therefore a robust secure network engineering process must be deployed to complement the detailed controls being measured in other sections of this document. Among the engineering/architectural standards to be used are:

1. Config/Hygiene: To support rapid response and shunning of detected attacks, the network architecture and the systems that make it up should be engineered for rapid deployment of new access control lists, rules, signatures, blocks, blackholes and other defensive measures required by US-CERT.

2. Vis/Attrib: All access of websites on the Internet must occur through a perimeter that includes a firewall, IDS, web proxy, packet inspection, packet logging functionality and session reconstructor abilities.

3. Vis/Attrib: DNS should be deployed in a hierarchical, structured fashion, with all client machines sending requests to DNS servers inside a government-controlled network and not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers that are allowed to send requests to the Internet.

4. Config/Hygiene: Each organization should standardize the DHCP lease information and time assigned to systems, and verbosely log all information about DHCP leases distributed in the organization.

## Critical Control 17: Red Team Exercises

**How do attackers exploit the lack of this control?**

Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware.  Once they get access, they burrow deep and expand the number of systems over which they have control.  Most organizations do not exercise their defenses so they are uncertain about its capabilities and unprepared for identifying and responding to attack.

This control goes beyond traditional penetration testing, which typically has the goal of identifying vulnerabilities and showing their business risks. Red Team Exercises are exercise in the traditional sense of military exercises where the three goals are improved readiness of the organization, better training for defensive practitioners, as well as inspection of current performance levels.  Independent red teams can provide valuable objectivity regarding both the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even those planned for future implementation.

**How can this control be implemented and its effectiveness measured?**

1. Vis/Attrib: Conduct exercises to test the readiness of organizations to identify and stop attacks or to respond quickly and effectively.
2. Vis/Attrib: Ensure systemic problems discovered in Red Team exercises are fully mitigated.
3. Vis/Attrib: Measure, in particular how well the organization has reduced the significant enablers for the attacker (these are all counted on by Red Teams) by setting up automated processes to find:
   - Cleartext emails and docs with "password" in the filename or body.
   - Critical network vsd diagrams stored online and in cleartext
   - Critical config files stored online and in cleartext.
   - Assessment documents stored online and in cleartext.
   - Cleartext protocol use internal and external to the network (telnet, FTP, etc.)
4. Advanced: Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.
5. Advanced: Create a test bed that mimics a production environment for specific Red Team attacks against elements that are not typically tested in production, such as attacks against SCADA and other control systems.

# Critical Control 18:  Incident Response Capability

A great deal of damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response programs in place.

The National Institute of Standards and Technology (NIST) has released detailed guidelines for creating and running an incident response team in Special Publication 800-61, available at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.   Among the most important elements included in these guidelines are:

1. QW: Develop written incident response procedures, which include a definition of personnel roles for handling incidents.  The procedures should define the phases of incident handling consistent with the NIST guidelines cited above.
2. QW: Assign specific individuals job titles and duties for handling computer and network incidents.
3. QW: Define management personnel that will support the incident handling process within each organization, acting in key decision-making roles
4. QW: Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the agency incident handling team, the mechanisms for such reporting, and the kind of information that should be passed in the incident notification.  This reporting should also include notifying US-CERT in accordance with federal requirements for involving that organization in computer incidents.
5. QW: Publish information to all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Include such information in routine employee awareness activities.
6. Config/Hygiene: Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that personnel understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

# Critical Control 19:  Data Recovery Capability

**How do attackers exploit the lack of this control?**
When attackers compromise machines, they often make significant changes to configurations and software.  Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information.  When the attackers' presence is discovered, organizations without a trustworthy data recovery capability can have extreme difficulty removing all aspects of the attacker's presence on the machine.

**How can this control be implemented and its effectiveness measured?**

1. QW: Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information.   To help ensure the ability to

rapidly restore a system from backup, make sure that the operating system, application software, and data on a machine are each included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or using the same backup software. However, each must be backed up at least weekly.

2. Config/Hygiene: Ensure that backups are encrypted when they are stored locally, as well as when they are moved across the network.
3. Config/Hygiene: Backup media, such as hard drives and tapes, should be stored in physically secure, locked facilities.

**Procedures and tools for implementing this control:**
Once per quarter, a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

# Critical Control 20: Security Skills Assessment and Appropriate Training To Fill Gaps

The skills of five groups of people are constantly being tested by attackers:
1. End users are fooled into opening attachments and loading software from untrusted sites, visiting web sites where they are infected and more.
2. System administrators are also fooled like normal users but are also tested when unauthorized accounts are set up on their systems, when unauthorized equipment is attached, when large amounts of data are exfiltrated.
3. Security operators and analysts are tested with new and innovative attacks with sophisticated privilege escalation, with redirection and other attacks along with a continuous stream of more traditional attacks.
4. Application programmers are tested by criminals who find and exploit the vulnerabilities they leave in their code.
5. To a lesser degree system owners are tested when they are asked to invest in cyber security but are unaware of the devastate impact a compromise and data exfiltration or data alteration would have on their mission.

Any organization that hopes to be ready to find and respond to attacks effectively owes it to their employees and contractors to find the gaps in their knowledge and to provide exercises and training to fill those gaps. A solid security skills assessment program can provide actionable information to decision makers about where security awareness needs to be improved, and can also help determine proper allocation of limited resources to improve security practices.

**How can this control be implemented and its effectiveness measured?**

1. QW: Develop security awareness training for various personnel job descriptions.  The training should include specific, incident-based scenarios showing the threats an organization faces.

2. Config/Hygiene: Devise periodic security awareness assessment quizzes, to be given to employees and contractors on at least an annual basis, determining whether they understand the information security policies and procedures for the organization, as well as their role in those procedures.

3. Config/Hygiene: Conduct periodic exercises to verify that employees and contractors are fulfilling their information security duties, by conducting tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller.

**Procedures and tools for implementing this control:**
The key to upgrading skills is measurement – not with certification examinations, but with assessments that show both the employee and the employer where knowledge is sufficient and where the gaps are.  Once the gaps are identified, those employees who have the requisite skills and knowledge can be called upon to mentor the employees who need skills improvement or the organization can develop training programs that directly fill the gaps and maintain employee readiness.

## SUMMARY

This document has been developed through the collaboration of a diverse set of security experts.  While there is no such thing as absolute protection, proper implementation of the security controls identified in this document will ensure that an organization is protecting against the most significant attacks.   As attacks change, as additional controls or tools become available, or as the state of common security practice advances, this document will be updated to reflect what is viewed by the collaborating authors as the most important security controls to defend against cyber attacks.

## Appendix A: Initial mapping between CAG 097 control set and
## draft NIST SP 800-53 Rev 1, 2/9/2009

This mapping relays the SP 800-53 Rev 3 controls which accomplish the requirements called out in the CAG 097 control set. Note that for the most part, where the CAG 097 control set called for a requirement not currently in the draft for SP 800-53 Rev 3, an enhancement was added to the NIST draft to cover that requirement. Also note that the NIST controls may impose additional requirements beyond those explicitly stated in CAG 097.

| CAG 0 97 Control | Related NIST SP 800-53 Rev 3 Controls |
|---|---|
| Critical Control 1: Inventory of authorized and unauthorized hardware. | CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9 |
| Critical Control 2: Inventory of authorized and unauthorized software; enforcement of white lists of authorized software. | CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7 |
| Critical Control 3: Secure configurations for hardware and software for which such configurations are available. | CM-6, CM-7, CP-10, IA-5, SC-7 |
| Critical Control 4: Secure configurations of network devices such as firewalls, routers, and switches. | AC-4, CM-6, CM-7, CP-10, IA-5, RA-5, SC-7<br>(Also related to assessment with SP 800-53A) |
| Critical Control 5: Boundary Defense | AC-17, RA-5, SC-7, SI-4<br>(Also related to assessment with SP 800-53A) |
| Critical Control 6: Maintenance, Monitoring and Analysis of Complete Audit Logs | AU-1, AU-2, AU-3, AU-4, AU-6, AU-7, AU-9, AU-11, AU-12, CM-3, CM-5, CM-6, SI-4<br>(Also related to assessment with SP 800-53A) |
| Critical Control 7: Application Software Security | AC-4, CM-4, CM-7, RA-5, SA-3, SA-4, SA-8, SA-11, SI-3 |
| Critical Control 8: Controlled Use of Administrative Privileges | AC-6, AC-17, AT-2, AU-2 |
| Critical Control 9: Controlled Access Based On Need to Know | AC-1, AC-2, AC-3, AC-6, AC-13<br>(Also related to assessment with SP 800-53A) |
| Critical Control 10: Continuous Vulnerability Testing and Remediation | CA-2, CA-6, CA-7, RA-5, SI-2 |
| Critical Control 11: Dormant Account Monitoring and Control | AC-2, PS-4, PS-5 |
| Critical Control 12: Anti-Malware Defenses | AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8 |
| Critical Control 13: Limitation and Control of Ports, Protocols and Services | AC-4, CM-6, CM-7, SC-7<br>(Also related to assessment with SP 800-53A) |
| Critical Control 14: Wireless Device Control | AC-17 |

| | |
|---|---|
| Critical Control 15: Data Leakage Protection | AC-2, AC-4, PL-4, SC-7, SC-31, SI-4 |
| Critical Control 16: Secure Network Engineering | AU-8, CA-2, CA-6, CM-7, SA-8, SC-7, SC-22 |

| | |
|---|---|
| Critical Control 17: Red Team Exercises | CA-2, CA-6 |
| Critical Control 18: Incident Response Capability | IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, SI-5 |
| Critical Control 19: Disaster Recovery Capability (Control is TBD – still under development) | CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10 (likely based upon CAG 097 control title) |
| Critical Control 20: Security Skills Assessment and Appropriate Training To Fill Gaps | AT-2, AT-3, AT-4 |