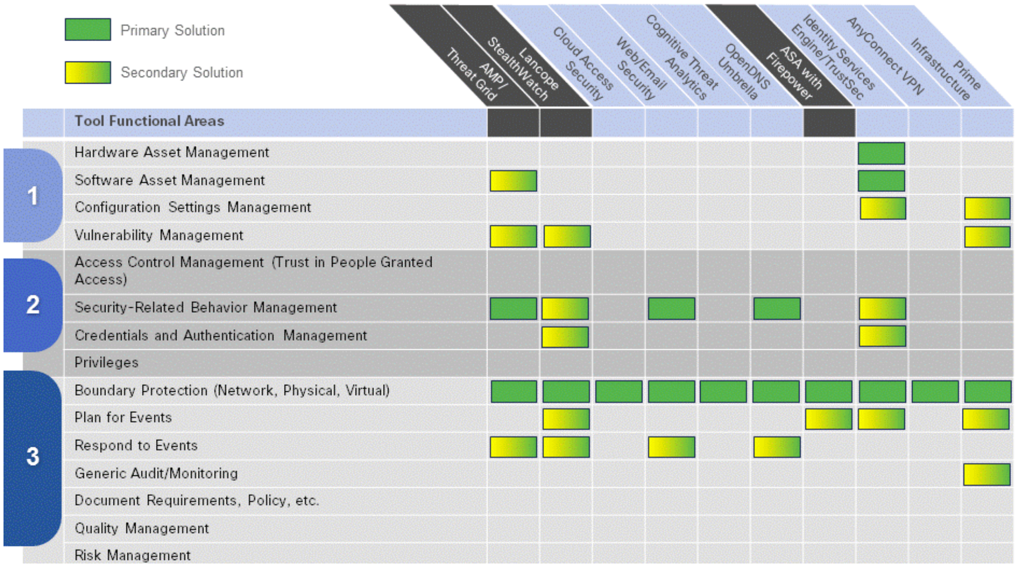
Cisco Provides Essential Cyber Solutions for Continuous Diagnostics and Mitigation

The US Department of Homeland Security (DHS) developed the Continuous Diagnostics and Mitigation (CDM) Program to help federal agencies bolster their cyber defenses. The CDM Program offers products and services across multiple security disciplines to prioritize and fix critical cyber weaknesses. This paper explains how Cisco's cybersecurity solutions are essential for the CDM Program – and to manage security risks across the full attack continuum.

Cisco Solutions for CDM

Cisco offers a complete set of solutions for the CDM Program including policy and access controls, next-gen network security, advanced threat solutions, and content security capabilities. Table 1 summarizes:

Table 1. Summary of Cisco Cybersecurity Solutions for CDM



🟩 Primary Solution

🟨 Secondary Solution

	Tool Functional Areas	AMP/ Threat Grid	Lancope StealthWatch	Cloud Access Security	Web/Email Security	Cognitive Threat Analytics	OpenDNS Umbrella	ASA with Firepower	Identity Services Engine/TrustSec	AnyConnect VPN	Prime Infrastructure
1	Hardware Asset Management								🟩		
	Software Asset Management	🟨							🟩		
	Configuration Settings Management								🟨		🟨
	Vulnerability Management	🟨	🟨								🟨
2	Access Control Management (Trust in People Granted Access)										
	Security-Related Behavior Management	🟩	🟨		🟩		🟩		🟨		
	Credentials and Authentication Management		🟨						🟨		
	Privileges										
3	Boundary Protection (Network, Physical, Virtual)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Plan for Events		🟨					🟨	🟨		🟨
	Respond to Events	🟨	🟨		🟨		🟨				
	Generic Audit/Monitoring										🟨
	Document Requirements, Policy, etc.										
	Quality Management										
	Risk Management										

The Cisco Cybersecurity Portfolio

Cisco Solutions for Policy and Access

- **Cisco Identity Services Engine (ISE)** - The all-in-one enterprise policy control platform that enforces compliance, enhances infrastructure security, and simplifies service operations.
- **Cisco TrustSec** - Software-defined segmentation that simplifies the provisioning of network access, accelerates security operations, and consistently enforces policy anywhere in the network. Cisco TrustSec is embedded technology in Cisco switches, routers, wireless and security devices and is a part of the Network-as-an-Enforcer solution.
- **Cisco AnyConnect Secure Mobility Client** - The enhanced remote access VPN solution that makes user connectivity easier and more secure.

Cisco Solutions for Next-Generation Network Security

- **Cisco Next-Generation Firewall** - The new, adaptive threat-focused next-generation firewall that delivers superior, multi-layered protection, improves visibility, and reduces security costs and complexity.
- **Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS)** - The critical part of an organization's overall network and systems protection strategy that provides essential defense-in-depth capabilities.

Cisco Solutions for Advanced Threat Protection

- **Cisco Advanced Malware Protection (AMP) + AMP Threat Grid** - The only malicious code protection solution that combines the power of big data analytics, point-in-time detection, and retrospective security (continuous analysis) capabilities.
- **Cisco Lancope StealthWatch** - The network flow analysis solution that baselines normal network traffic and spots anomalous or suspicious activity, improving network visibility, security, and response.

Cisco Solutions for Content Security

- **Cisco OpenDNS Umbrella** - The solution that creates a new DNS layer of cloud-delivered protection in the network security stack, both on and off the corporate network. Umbrella prevents command and control callbacks, malware, and phishing over any port or protocol.
- **Cisco Cloud Access Security (CAS)** - The cloud app security solution that monitors usage in real time and extends essential controls into cloud applications like Box or Dropbox, vectors for possible data loss.
- **Cisco Cognitive Threat Analytics** - The solution that turns the web proxy into a security sensor that automatically identifies and investigates suspicious web-based traffic, and alerts on confirmed breached devices.
- **Cisco Email and Web Security** - Email security capabilities include spam filtering, data loss protection, anti-malware protection, dynamic encryption, and privacy filters. Web security capabilities include multiple anti-virus analysis engines, reputation-based filtering, application visibility and control, and data protection.

Cisco Solutions for Simplified Management

- **Cisco Prime Infrastructure** - The solution that simplifies the management of wireless and wired networks from the branch to the data center. Cisco Prime “One Management” consolidates and reduces the number of tools required to manage the network, and monitors and troubleshoots Cisco ISE policy as well.

- **Cisco Firepower Management Center** - The administrative nerve center for Cisco network security solutions. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

Selecting the Right CDM Partner

The CDM Program seeks to provide federal agencies with modern, commercial off-the-shelf (COTS) cybersecurity tools that can adapt to the ever-changing threat landscape. But to successfully fulfill this mandate, an agency's CDM partner must understand the program's goals and empower their own solutions with three critical capabilities: **integration**, **consolidation** and **automation**. At Cisco, we understand this and believe these three capabilities are the best way to enhance cybersecurity without increasing complexity. We also understand that the need for simplicity and scalability is especially true with the current shortage of cyber professionals in federal government. So when considering your partner for CDM, you can rest assured that Cisco has you covered.

Integration

Cisco cybersecurity solutions are designed to integrate seamlessly and share information in real time. Consider the following proof points:

- **Cisco is Visibility-Driven** - Visibility is at the heart of Cisco's security strategy. It means that our solutions can detect the hardware and software on your network to build asset inventories and remove unauthorized devices and applications. Contextual information like user name, operating system, hardware type and vulnerability information is shared for event correlation and prioritization. We believe visibility is central to any cybersecurity strategy because you can't protect what you can't see.
- **Cisco is Platform-Based** - Cisco solutions are agile and open. That they are built for scale, consistent control, and ease of management. That means we have developed a partner ecosystem to embed security into broader IT solutions and to make security an enabler. For example, Cisco ISE integrates with our ecosystem partner, Ping Identity, to provide users with federated single sign-on to both in-house and cloud applications. This eliminates the need for password list which can be easily compromised and is just one example of how the Cisco Platform Exchange Grid (pxGrid) can deliver multivendor, cross-platform integration.
- **Cisco is SCAP-Enabled** - Cisco understands that support for the Security Content Automation Protocol (SCAP) is essential for CDM solution integration. That's why, back in 2012, our Product Security Incident Response Team (PSIRT) began including Open Vulnerability and Assessment Language (OVAL) definitions in Cisco IOS security advisories. OVAL is part of the SCAP suite and accelerates the best practices for vulnerability and configuration management. So our partner ecosystem includes security information and event management (SIEM) vendors who support SCAP.

Consolidation

When it comes to determining cybersecurity solutions, quantity is not necessarily the best approach. In fact, it may be the opposite. More products bring more user interfaces, more configurations to manage and more systems to monitor. This raises complexity and can even hamper the successful implementation of many product features. And since most federal agencies are already short-staffed, adding more administrative and analysis burden to overloaded federal cyber pros can do a great deal of harm and actually reduce an agency's cybersecurity in the long run. That's why we believe solution consolidation is key. Consider the following proof points:

- **Cisco means Security Everywhere** - Security is embedded in everything we do. We include our Advanced Malware Protection capabilities in our network security solutions, our email and web security solutions (and even our AnyConnect VPN client). No need to buy and install a separate product since the capabilities are built-in. Plus Cisco's Simplified Management solutions consolidate management user interfaces for consistent control across products. We've even extend our Firepower NGIPS into the Cisco Integrated Services Router (ISR). It's called Firepower Threat Defense for ISR and combines best-in-class threat protection with our industry-leading converged branch routing platform.
- **Cisco means Security-As-A-Service** - Many of our cybersecurity solutions are available as a service from the cloud, including OpenDNS, Cloud Web Security, Cognitive Threat Analytics and Cloud Access Security. All of our solutions are backed by Cisco Talos, our industry-leading threat research organization that delivers threat intelligence to your Cisco Security solutions through the cloud. This means less hardware to buy, manage and operate as it consolidates operations through the Cisco Powered Cloud.

Automation

The CDM Program is meant to automate data collection as well as automatically identify the most critical security problems at the agency level. It feeds summary information into an enterprise-level dashboard for near real-time situational awareness and cybersecurity risk posture assessment across the federal government. Consider the following proof points:

- **Cisco means Better Data –** As devices connect and disconnect, data speeds across networks and information is shared, the threat of compromise increases. It is a fast moving world of constant threats. At Cisco, our solutions reduce dependence on human beings to recognize these threat by automatically seeking out intrusions or security risks and pre-emptively arming your network against them. Our solutions help ensure the reliable and secure sharing of a variety of data 24/7, end-to-end so that data is not compromised and critical services can go on interrupted.
- **Cisco means Improved Workflow –** The key to responding holistically to attacks is providing an automated security response. This allows streamlining of existing workflows so that limited resources, both physical and financial, can be better prioritized and allocated. It also improves efficiency by directly linking security information and event management tools to workflows.
- **Cisco means Faster Response –** It is often easy to spot cyber threats but far more difficult to respond to them correctly and efficiently. By continually monitoring for threats, our solutions speed response times to prevent or limit potential damage to networks and keep threats from spreading. By reducing the time between detection and response, Cisco's Threat-Centric solutions for cyber security help your networks and users stay up and running. This increases productivity and improves government services for citizens while also keeping our nation's data safer, especially in times of emergency.
- **Cisco means Better Morale –** Government cyber defenders often find themselves overwhelmed by too much information, constantly evolving threats and an outdated response. Add to that any regulatory requirements and the morale of personnel can suffer greatly. By automating time consuming and repetitive aspects of cyber security, such as network traffic monitoring or filtering thru data, this burden is greatly reduced. Personnel can then be alerted as they feel necessary and freed to pursue other priorities, all while increasing security and response times.

Leveraging Cisco Solutions for CDM

The initial phase of CDM focuses on four functional capabilities: hardware management, software management, configuration, and vulnerability. These are considered baseline capabilities to protect data. But an end-to-end model with automated analytics is required to provide network, security and risk management teams with a firm understanding of where security is working, where investment is needed and where their greatest risks of attack lie. Known as **Security Intelligence**, this wealth of information enables organizations to allocate resources where needed most, embed best practices into daily operations and take prioritized action when needed.

How Cisco ISE Benefits Government Agencies

Advancing Effeciency:

- Management + security from a single solution
- Broad breadth of management
- Comprehensive Security
- Manages and secures virtually all enterprise device types
- Optimized for remote environments
- Integrated with desktop management
- Market-leading technology

Reducing Costs:

- Cost reduction — $ and IT resources
- Reduced number of support contracts to maintain
- Lowered mobile device TCO through elimination of vendor redundancies
- Single multi-channel access gateway for mobility

Simplifying Management:

- Single console to manage and secure laptops and mobile devices
- Management and security tasks occur in a single connection
- Integrated platform means solution will seamlessly work together: no need to “manage the gaps”
- Improved technical product support
- Reduced end-user device complexity

Empower a Threat-Centric Approach for CDM

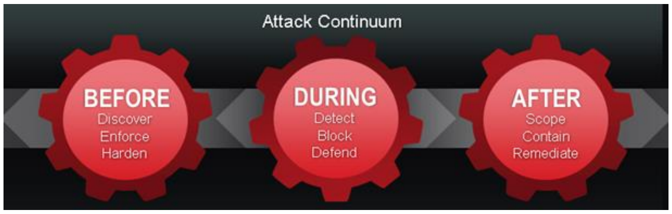
Cisco is unique in its capability to deliver the threat-centric approach to security essential to safeguarding sensitive information and protecting our nation’s networks. Cisco’s new security model reduces complexity while providing superior visibility, continuous control, and advanced threat protection across the entire attack continuum – before, during, and after an attack.

The **Cisco® Identity Services Engine (ISE)** actively identifies and classifies hardware that attempts to connect to the network, and blocks hardware that is not authorized to connect. It leverages network infrastructure investments for rapid, scalable asset detection and profiling. Plus an automated device feed service updates Cisco ISE in real time to help ensure that new devices can be identified as soon as they are released to the market. When combined with Cisco FireSIGHT, a powerful solution that can provide total, real-time network visibility and security, you can gain even greater threat detection and quarantine capability. FireSIGHT passively discovers and inventories all hardware that connects to the network -- including servers, systems, virtual hosts, and mobile devices -- so that any unmanaged hardware can be quickly identified and removed.

The **Splunk for Cisco ISE** add-on allows for the extraction and indexing of the ISE AAA Audit, Accounting, Posture, Client Provisioning Audit and Profiler events. This integration allows any Splunk user to correlate ISE data with other data sources (e.g. with firewall events or application data) to get deeper operational and security visibility. It also includes sample dashboards and reports for profiling, authentication, system statistics, alarms and location awareness. Cisco ISE is also designed to integrate with Qualys, Tenable and Rapid 7 to provide enhanced assessment reporting. To learn more about Splunk, visit: https://splunkbase.splunk.com/app/1589/.

Span the Entire Attack Continuum

Before an attack occurs, departments and agencies must discover the hardware and software that they have, enforce the proper access controls, and harden critical assets to reduce the attack surface area. **During** an attack, they must immediately detect that an attack is in progress so they can block and defend against it. **After** the attack they must scope the breach so that they can contain damage, remediate to restore proper system operation and prevent recurrence. For these reasons, Cisco offers a comprehensive portfolio of threat-centric cyber security solutions that span the entire attack continuum.



The goals of the DHS CDM program align closely with Cisco's New Security Model. For example, the Hardware Asset Management and Software Asset Management functional areas discover unmanaged hardware, software, and malicious code to prevent attacks (Phase 1 – Before). The Manage Security Related Behavior function detects potentially suspicious or risky activity, blocks insider threats from being successful, and defends against attackers' attempts to exploit insiders or internal vulnerabilities while they are in process (Phase 2 – During). The Respond to Contingencies and Incidents function responds swiftly to end ongoing attacks and limit the damage – critical "After" phase capabilities to recover from an attack (Phase 3 – After).

Implement Baseline Security for Individual Devices

Cisco ISE's superior device profiling and "zero-day" device profile feed service, provides updated profiles for the latest devices. Combined, these two features help reduce the number of unknown endpoints (and potential threats) on an agency network. Once unauthorized or unmanaged hardware is discovered by ISE, the department or agency (D/A) will need to take action to remove the hardware. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.

Ensure Security for the End-to-End Network

The Cisco NAC Appliance is a product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, IP phones, personal digital assistants, or printers are compliant with an organization's security policies, and repairs any vulnerabilities before permitting access to the network. Other technology companies, such as Symantec, Trend Micro, and McAfee, have recently introduced solutions that enforce policies on individual endpoints; but the Cisco NAC Appliance is much different.

The NAC Appliance covers the entire lifecycle of policy enforcement: authentication, posture assessment, network quarantine and remediation. Cisco can offer this robust, integrated set of features because the NAC Appliance uses the network as the enforcement point rather than individual endpoints. As a result, Cisco NAC solutions are more effective and integrate into the network fabric with greater ease than an endpoint-based approach.

Look at Overall Risk

Adaptive Network Control (ANC) is a service that runs on the Cisco ISE Administration node to extend the monitoring and controlling of endpoints. ANC allows you to reset the network access status of an endpoint to:

- **Quarantine -** use policies to disallow an endpoint access to the network or limits its access. Policies can be created to assign different authorization profiles depending on the status.

- **Unquarantine -** reverse the quarantine status, allowing the endpoint full access to the network.
- **Shutdown -** deactivate a port on the network attached system (NAS). Once a port is shutdown, it has to be manually reset.

For example, upon discovery of a hostile endpoint on your network, you can shut down the endpoint's access by using ANC to close the NAS port. It can also be used to change the authorization state without having to modify the overall authorization policy of the system. ANC supports both wired and wireless deployments.

Other Solution Areas Supported

With a slew of acquisitions of cutting edge security firms, such as Sourcefire, Cisco products are well positioned to handle correlation, context, and visualization of information layered on top of metrics that can make practical and dramatic changes to security. For example, adding Sourcefire's Advanced Malware Protection (AMP) technology into the email and Web security appliances has resulted in AMP using file reputation and sandboxing. AMP also uses a technique called file retrospection for analyzing threats that have made it into the network. File retrospection monitors and tracks user devices that have been exposed to malware so that a company can take steps to remediate the problem. This allows agencies to comply with all three phases of the DHS CDM initiative.

Cisco's FirePOWER Next-Generation IPS (NGIPS) solution also advances the federal CDM goals by setting a new standard for advanced threat protection. FirePOWER does this by integrating:

- Real-time contextual awareness
- Intelligent security automation
- Superior performance with industry-leading network intrusion prevention.

Cisco also focuses on boundary protection and network access control, areas that ISE can centralize policy for.

- See: http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

When a network admin executes a traditional ACL list in a large network, one could find over 2000+ lines of non-descript ACL policies, most of which were added by a prior administrator without any clear association on why each rule was added. Using this traditional model, performing network wide audits on access policies becomes extremely difficult if not impossible to achieve with limited IT staff.

Using ISE with TrustSec allows for a centralized human-readable policy that makes auditing network wide policy achievable, even with limited IT staff. Agencies are also moving towards Software Defined Networks (SDN) to improve the speed of their IT operations. ISE/TrustSec works in this framework, with solutions like APIC EM.

- See: http://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-enterprise-module/index.html

Summary

With the ongoing implementation of the DHS CDM program, federal organizations are one step closer to an effective, resilient cyber defense posture. But these security controls must be more than just a compliance exercise. They must be part of a broader effort to advance the operational missions of federal agencies by reducing overall risks by establishing an all-encompassing and continuous panoramic view of the network. Instead of looking for malicious files, registry entries or configuration changes, continuous monitoring systems must now look for network behavior patterns. By creating a common platform to manage risk, leveraging existing third-party technologies, and turning disparate data streams into actionable intelligence, agencies can achieve full implementation of the prioritized Critical Controls and move quickly towards long-term risk management maturity.

Cisco cybersecurity solutions uniquely deliver the essential, threat-centric Continuous Diagnostic and Mitigation capabilities that secure government networks – before, during, and after an attack. Cisco is in a unique position to deliver the essential, threat-centric continuous diagnostic and mitigation capabilities that can secure government networks before, during, and after an attack. Whether you're a Blanket Purchase Agreement awardee delivering on critical CDM functions, or a department or agency seeking the right CDM tools, by selecting Cisco cyber security solutions to power your technology platform, you can secure your environment before, during, and after the coming attack.

Next Steps

To learn more about Cisco's US Government Solutions and Services, visit us at http://www.cisco.com/go/federal.

For more detailed information about Cisco's Cybersecurity Solutions for Continuous Monitoring and Mitigation, contact:

Brian Finan	Account Manager, Security Sales
Email:	brfinan@cisco.com

Appendix A

CDM Primary Solution Areas

Manage Network Access Controls

To prevent attackers from exploiting internal and external network boundaries, departments and agencies must remove and limit unauthorized network connections and access. This can be achieved using:

- **Cisco ISE and TrustSec** to deliver identity-aware logical network segmentation and access policy enforcement where the network enforces logical access policies itself.
- **Cisco ASA with FirePOWER Services** to provide comprehensive boundary controls through the industry's first threat-focused, fully integrated next-gen firewall and IPS.
- **Cisco Email Security Appliance (ESA), Web Security Appliance (WSA), and Advanced Malware Protection (AMP) and OpenDNS Umbrella** to control harmful connections, content and quarantine advanced malware.
- **Cisco AnyConnect** to offer scalable, secure remote access for mobile workers through next-generation security controls and advanced encryption.
- **Cisco Prime** for managing enterprise-wide access control lists on network boundaries.

Manage Security-Related Behavior

To prevent both privileged and general users from taking unnecessary security risks, departments and agencies must monitor individuals for potentially suspicious or risky activity, prevent insider threats from being successful, and block attackers from exploiting insiders or internal vulnerabilities. This can be achieved using:

- **Cisco ESA, WSA, AMP and OpenDNS Umbrella** to control harmful connections and quarantine advanced malware that can dupe insiders though social engineering attempts or can exploit vulnerable systems.
- **Lancope StealthWatch** to detect internal security risks such as policy violations and data leakage attempts through sophisticated host and network behavioral analysis of Cisco NetFlow, Internet Protocol Flow Information Export (IPFIX) and other network traffic flow data.

Hardware Asset Management

Since unauthorized or unmanaged hardware is likely to be vulnerable, unpatched, and/or carry malicious code that can introduce security risks, departments and agencies must identify unmanaged hardware for immediate removal. This can be achieved using:

- **Cisco Identity Services Engine (ISE)** which actively identifies and classifies hardware that attempts to connect to the network, and blocks hardware that is not authorized to connect. It leverages network infrastructure investments for rapid, scalable asset detection and profiling. An automated device feed service updates Cisco ISE in real time to help ensure that new devices can be identified as soon as they are released to the market.

Supporting Solution Areas

Software Asset Management

Since unauthorized or unmanaged software is likely to be vulnerable, unpatched, and/or carry malicious code that can introduce security risks, departments and agencies must identify and unmanaged software -- especially malware -- for immediate removal. This can be achieved using:

- **Cisco Advanced Malware Protection (AMP)** to identify and quarantines malicious code, the worst form of unauthorized or unmanaged software. It operates at all points where malware attempts entry: through the network itself, through endpoint systems including mobile devices, and through web and email content.

Configuration Settings Management

Over 80% of known vulnerabilities are attributed to misconfiguration and missing patches, so departments and agencies must ensure proper configuration of all IT assets including hardware, software, and virtual machines. This can be achieved using:

- **Cisco Prime** which provides comprehensive management for Cisco network assets through a single pane of glass view. It archives, versions, and compares configurations to detect and report changes or mismatches. It rolls configurations back to prior, known-good baselines if future configuration changes or mistakes violate policy or cause sec/ops issues.
- **Lancope StealthWatch** for detecting abnormal network traffic patterns that are often telltale signs of system misconfigurations.

Vulnerability Management

Weaknesses in software are subject to exploitation, and can be leveraged to launch attacks affecting other critical systems. For these reasons, departments and agencies must manage the risks associated with known software weaknesses. This can be achieved using:

- **Cisco Advanced Malware Protection (AMP)** which mitigates the potential damage caused by malware that exploits system vulnerabilities, both at a given point in time and continuously. Its retrospective analysis uses the very latest information to update dispositions and quarantine malicious code even after it reaches end points.
- **Cisco Prime** for helping to identify misconfigured devices by ensuring that all configurations are properly set, thereby mitigating vulnerabilities.
- **Lancope StealthWatch** to detect abnormal network traffic that can result from vulnerabilities.

Manage Credentials and Authentication

Departments and agencies must ensure that account credentials are assigned to and used by authorized individuals to help prevent credentials from being used by anyone other than the authorized owner. This can be achieved using:

- **Cisco ISE** to deliver comprehensive Authentication, Authorization, and Accounting (AAA) capabilities to help manage credentials and authentication.

Prepare for Contingencies and Incidents

To be prepared for attacks and unanticipated events, to prevent attackers' compromises from being effective by being adequately planned to respond, and to prevent natural disasters and other unforeseen incidents from disrupting the mission are all critical aspects of this functional area. This can be achieved using:

- Cisco's "Before" phase solutions that include **Cisco ASA with FirePOWER Services, Cisco ISE, Cisco TrustSec, Cisco AnyConnect and OpenDNS** to discover, enforce, and harden – vital preparatory controls for the inevitable, advanced threats that will face agency and department networks.
- **Lancope StealthWatch** which collects, analyzes, and stores network traffic data for months – or even years -- to facilitate incident investigations.

Respond to Contingencies and Incidents

To learn from previous incidents, to limit the impact of ongoing incidents, to appropriately respond to end ongoing attacks, and to identify ways to prevent recurrence are all crucial aspects of this functional area. This can be achieved using:

- Cisco's "During" phase solutions which include **Cisco Next Generation IPS, Cisco ESA, Cisco WSA and OpenDNS Umbrella** to detect, block, and defend against in-progress attacks.
- Cisco's "After" phase solutions that include **Cisco Advanced Malware Protection (AMP) and OpenDNS Investigate** to scope, contain, and remediate attacks that may have already succeeded.

Manage Audit Information

Departments and agencies must prevent attacks by using audit information to identify weakness and initiate an appropriate response. This can be achieved using:

- **Cisco Prime** which provides a single, unified view of all user access audit data to facilitate access suitability behavioral analysis and investigations.
- **Lancope StealthWatch** for providing a full audit trail of all network transactions for detecting anomalous traffic, suspicious activity, and performing more effective forensic investigations.

Appendix B

Additional Resources & References

ISE Data Sheets and Documentation

http://www.cisco.com/c/en/us/products/security/identity-services-engine/literature.html

ISE Design Guide

The Profiling document has the best information related to CDM HWAM). Also, see the information on PxGrid at the bottom, including the last one which list details on Splunk integration. This type of integration can be used in any phase to remove a device/user from the network. This will be a bigger part of Phase III.

http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html

Additional details on profile configurations

http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010100.html

DHS CDM Initiative

http://www.dhs.gov/cdm

Security Content Automation Protocol (SCAP)

NIST SCAP guidelines: http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf
SCAP Certified Tools: https://nvd.nist.gov/SCAP-Validated-Tools/
Tenable Integration: http://www.tenable.com/products/nessus/integrations/cisco-ise
Tenable SCAP Support: http://static.tenable.com/documentation/Nessus_5.2_SCAP_Assessments.pdf
Rapid7 Integration: http://www.rapid7.com/docs/CiscoISE-integration.pdf
Rapid7 SCAP Support: http://www.rapid7.com/solutions/compliance/fisma.jsp

DHS Information Sharing Specifications (STIX, TAXII etc.)

https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**