WHITE PAPER

Deep Dive: NIST SP 800-171r1 and DRAFT NIST SP 800-172 Compared

27 Oct 2020
Jason McNew, CISSP
Senior Engineer, Cybersecurity Risk & Compliance
Appalachia Technologies, LLC
jason.mcnew@appalachiatech.com

www.appalalachiatech.com
(717) 918-3301

Table of Contents

Purpose

The purpose of this whitepaper is an in-depth comparison of:

- NIST SP 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

TO

- DRAFT NIST 800-172 *Enhanced Security Requirements for Protecting Controlled Unclassified Information*

This white paper was not written to be extremely technical and is intended for both security professionals who work with NIST 800-171, as well as managers and executives overseeing compliance efforts. NIST 800-172 replaces the obsoleted NIST 800-171B. It is important to note that 800-172 (July 2020) is in DRAFT form at the time this white paper was published.

The biggest change we noticed between 800-171B and 800-172, is that much of the prescriptive language has been removed and replaced with "organizationally defined." For example, the mandate to have a yearly penetration test and the mandate for onsite incident response within 24 hours have both been replaced with "organizationally defined."

Background

NIST 800-172 contains 33 enhanced requirements beyond the original 110 controls in 800-171. The basic rational for 800-172 is summed up in the "Notes to Reviewers" section of that draft document:

> "This publication provides a set of enhanced security requirements to protect the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations from the advanced persistent threat (APT). The APT is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using both cyber and physical attack vectors."
>
> "The APT pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives."

The large prime contractors such as Lockheed Martin and General Dynamics already have highly evolved cybersecurity programs, so it is the remainder of the supply chain that is starting to get some MAJOR attention from the DoD where their cybersecurity (or lack of it) is concerned.

800-172 goes on to say:

> "The enhanced security requirements provide the foundation for a new multidimensional, defense-in-depth protection strategy that includes three, mutually supportive and reinforcing components: (1) penetration resistant architecture; (2) damage limiting operations; and (3) designing for cyber resiliency and survivability."

In other words, they are moving the DoD supply chain toward a more Risk Management based approach, by not only adding additional requirements for protective technologies, but also strategies to contain and limit the impact of breaches when they inevitably do happen. To that end, 171B contains mappings to the NIST CSF (Cybersecurity Framework), which is very useful to both executives and security managers.

Very importantly, NIST 800-172 correlates with levels four and five of the CMMC (Cybersecurity Maturity Model Certification.) Contractors who are required to be compliant at those levels can use NIST 800-172 as a framework.

Analysis

For each control family, we will begin with a brief high-level discussion of 800-171's original FIPS 200 derived basic requirements, followed by a description and explanation of 800-172's enhancements to those requirements. In some cases, we cite well-known vendors as solution examples – this is for demonstrative purposes only and should not be taken as an endorsement of those companies' products and/or services.

That said, let's get into the meat and potatoes of 800-172 here. Everything that really matters can be found in chapter three. As with the original 800-171, the new enhanced requirements are organized into 14 families – *Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection, and System and Information Integrity.* We'll go through the enhanced controls family by family.

3.1 Access Control

This family contains 2 basic requirements and 20 derived. The basic requirements are to:

- *Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).*

- *Limit system access to the types of transactions and functions that authorized users are permitted to execute.*

A properly designed and maintained standard business support system that is Windows based and following The 20 CIS Controls & Resources can meet most of this family without much additional effort or cost.

800-172 contains 3 enhanced security requirements beyond the first 22:

> 3.1.1e Employ dual authorization to execute critical or sensitive system and organizational operations.

Do not confuse this requirement with 2FA and MFA (dual and multi-factor authentication); they are not the same at all. What they are referring to here is TPI, or "Two Person Integrity". This means that two people are required when executing certain "commands, operations, or functions" – meaning those operations deemed to be the most critical to your organization.

> 3.1.2e Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.

Any BYOD (Bring Your Own Device) goes out the window with this one for sure. As it currently reads, this also seems to imply that cloud services can't be used, but when we dig into the guidance from 800-53, it qualifies that a little further and gives us the option to either *restrict* or *prohibit* the use of external information systems. There are many DoD contractors using cloud, but it has to be the right kind of cloud (such as Microsoft GCC or Google Government Cloud). This is also going to create some additional burdens where third party protective services such as SIEM and vulnerability scanning go.

> 3.1.3e Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.

Controlling the flow of CUI, especially in large organizations, can be very challenging. The first step in the process is usually a room full of people and a whiteboard, so that we can figure out

where all of the CUI actually ***is*** -- and that is just the beginning. We recently did exactly this with a large cloud company, and determined that CUI existed in AWS, Google, Azure, Jira, Salesforce, and numerous proprietary systems that existed outside of the facility that is supposed to be servicing the government. Controlling the flow of CUI (or any other important data) entails a complex mix of both technical and administrative controls.

The main takeaway from this one is that the original control is only mapped to the base portion of AC-4 in NIST 800-53, whereas the newly enhanced control is mapped to 7 additional sections of AC-4, plus SC-46 (Cross Domain Policy Enforcement). Meaning, that controlling the flow of your CUI properly is going to be MUCH more difficult under 800-172. This control enhancement alone could warrant an entire separate white paper.

3.2 Awareness and Training

This family contains 2 basic controls and 1 derived. The basic requirements are to:

- *Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems*.

- *Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.*

Under the original framework, contractors basically have to have a regular formal cyber security training program in place that includes insider threat training and incident response training. In larger organizations, this control is interpreted to mean that IT and security people should have training commensurate with their job roles. DoD Directive 8140 is a great reference for governing the last part.

800-172 contains 2 enhanced security requirements beyond the first 3:

> 3.2.1e Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.

This one is pretty self-explanatory. There are a bunch of vendors such as KnowBe4, Breach Secure Now, Wombat, etc. that contractors are using to train their people – while those are adequate under the original framework, 800-172 is demanding expanded training that is greater in depth.

3.2.2e Include practical exercises in awareness training for [Assignment: organization-defined roles] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.

Again, pretty self-explanatory. Here is what NIST 800-53 AT-2 has to say about this: "Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links."

3.3 Audit and Accountability

This family contains 2 basic requirements and 7 derived. The basic requirements are to:

- *Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.*

- *Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.*

Interestingly, 800-172 has NO new requirements here – a few words on that are in order here, however. Section 3.3 of the original framework basically mandates a system wide SIEM (Security Information and Event Monitoring) and in fact contains 9 of the 110 total controls -- about 8% of the total framework. If 8% of the framework is SIEM, we know this is something that the DoD takes very seriously. In spite of this fact, around 80% of the clients we have worked with do not have a SIEM at the outset of our assessments and have a tendency to drag their feet on SIEM post assessment. When a client is generally lacking protective technologies such as SIEM, IDPS, and vulnerability scanning, the best answer to that is usually a UTM (Unified Threat Management) solution.

3.4. Configuration Management

This family contains 2 basic requirements, and 7 derived. The basic requirements are to:

- *Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.*

- *Establish and enforce security configuration settings for information technology products employed in organizational systems.*

Many DoD contractors fall short on this and have limited written policies and procedures or configure their IT on an ad-hoc basis. ITIL (Information Technology Infrastructure Library) is a good resource for standing up a formal configuration management program.

800-172 contains 3 enhanced requirements beyond the first 9:

> 3.4.1e Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.

Well, this sounds kind of like the NSA's CSfC (Commercial Solutions for Classified Program) which is a lengthy list of COTS (Commercial Off The Shelf) hardware and software that has been vetted and approved for use on classified networks. Any easy way to meet this requirement would be to simply defer to the CSfC for all of your IT shopping needs and make it your company policy to do so. There are more than enough pre-approved products on the CSfC to build and maintain a full scope IT enterprise – I would not describe it as overly limiting.

> 3.4.2e Employ automated mechanisms to detect the presence of misconfigured or unauthorized system components; remove the components or place the components in a quarantine or remediation network that allows for patching, re-configuration, or other mitigations.

When Stronghold Cyber Security does assessments, there are often significant differences between what the customer thinks they have, and what they actually do have. The first answer to this problem is a robust vulnerability scanner similar to Nessus or Qualys, that can be used to discover unauthorized or misconfigured assets on your network. This control also warrants technology such as 802.1x or Kerberos to automatically restrict the connection of unauthorized or misconfigured assets. This kind of technology is not easy or cheap to maintain.

> 3.4.3.e Employ automated discovery and management tools to maintain an up-to -date, complete, accurate, and readily available inventory of system components.

Pretty self-explanatory. There are a bunch of advanced tools from various vendors that can do this. You need to know about EVERYTHING that is connected to your information systems at all times, and also receive notifications when unauthorized devices are connected for any reason.

3.5. Identification and Authentication

This family contains 2 basic requirements and 9 derived. The basic requirements are to:

- *Identify system users, processes acting on behalf of users, and devices*.

- *Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.*

Like 3.1 (Access Control), a properly designed and maintained standard business support system that is Windows based and following The 20 CIS Controls & Resources can meet most of this family without much difficulty – although if your infrastructure is cloud based vs. on premise, things are more complex.

800-172 contains 3 requirements beyond the first 11:

> 3.5.1e Identify and authenticate [Assignment: organization-defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.

The key word here is "BEFORE" establishing a network connection. Taken in conjunction with the enhancements in Configuration Management, this almost certainly means that 802.1x or similar is a must. In advanced environments, some contractors even use VPN ***internally.*** While impractical, using Wi-Fi along with RADIUS and WPA2 for everything in your environment would probably satisfy the intent of this control.

> 3.5.2e Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.

At first blush this control sounds like it is simply talking about a password manager like KeePass or LastPass, but that isn't the case. This means not using cheap network or security hardware that only supports a single administrator login and moving into enterprise level gear like HP and Cisco, along with TACACS+ (for example) to manage logins.

> 3.5.3e Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.

This control enhancement is working in conjunction with and reinforcing some of the others. The bottom line here is that being a Windows domain member and having MAC filtering in place are not good enough to be part of the information system – we also need advanced IAM (Identity and Access Management) along the lines of what RSA or Okta offer.

3.6. Incident Response

This family contains 2 basic requirements and 1 derived. The basic requirements are to:

- *Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities*.

- *Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.*

Under the original 800-171 framework, simply having a written Incident Response Plan, appointing some people to security roles and then testing that plan yearly was enough to satisfy the intent of the controls.

800-172 contains 2 requirements beyond the first 3.

> 3.6.1e Establish and maintain a security operations center capability that operates [Assignment: organization-defined time period].
>
> 3.6.2e Establish and maintain a cyber incident response team that can be deployed to any location identified by the organization within 24 hours.

They did loosen this up a bit from the obsoleted 800-171B, which seemed to imply a 24-hour SOC, and mandated on-site incident response within 24 hours. Apart from that, this does not require much explanation by the likes of us cyber security experts. Get out your check book.

3.7 Maintenance

This family contains 2 basic requirements and 4 derived. The basic requirements are to:

- *Perform maintenance on organizational systems*.

- *Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.*

A written set of policies and procedures (provided they are actually followed) is generally enough to satisfy the intent of this family. Interestingly, 800-172 doesn't add anything to this – regular maintenance is critical to the availability of information and information systems. The takeaway here is that like PCI and HIPAA, the DoD is more concerned with protecting the

confidentiality of the data than whether your business actually functions – something to keep in mind when implementing this framework. For that reason, it is a good idea to self-impose controls to address the availability of your information systems.

3.8 Media Protection

This family contains 3 basic requirements and 6 derived. *The basic requirements are to:*

- *Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital*, and to: *Limit access to CUI on system media to authorized users*.
- *Sanitize or destroy system media containing CUI before disposal or release for reuse.*

Removable media is a big risk in terms of data theft, especially where the insider threat is concerned. About half of the companies we have assessed under NIST 800-171r1 have no meaningful media protection (whether technical or administrative) in place at all.

We find it odd that 800-172 contains no enhancements, and we suspect that might change once its finalized. There should probably be some talk of DLP (Data Loss Prevention) technology in here.

3.9 Personnel Security

This family contains 2 basic requirements and no derived. The basic requirements are to:

- *Screen individuals prior to authorizing access to organizational systems containing CUI*.
- *Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.*

Most contractors screen their people at some level, whether it is using a third-party service such as ADP or doing criminal background checks, and that is all that the first version of 800-171 really required. It's also necessary to terminate system access and collect badges when someone is fired.

800-172 imposes 2 new requirements:

> 3.9.1e Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access on an ongoing basis.

3.9.2e Ensure that organizational systems are protected if adverse information develops about individuals with access to CUI.

It's not exactly clear on what the difference between a "personnel screen" and "enhanced personnel screening" means – although something along the lines of a NACI (National Agency Check with Inquiries) could eventually be imposed on everyone working in the Defense Industrial Base. In addition to the initial screening of new hires required under the original framework, 800-172 now requires keeping an eye on employees with access to CUI after hiring. This is another new requirement that won't be cheap.

3.10 Physical Protection

This family contains 2 basic requirements and 4 derived. The basic requirements are to:

- *Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals*.

- *Protect and monitor the physical facility and support infrastructure for organizational systems.*

Most contractors we have assessed have reasonable physical security controls in place, including a building access control system and building alarms. 800-172 has nothing to add here. The threat to CUI is mainly virtual, although there have been cases of insider persons working for our nations adversaries and stealing CUI and other critical data.

3.11 Risk Assessment

This family has only one basic requirement and 2 derived. The basic requirement is to:

- *Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.*

For smaller contractors, we simply include a Risk Assessment template as part of the SSP, and have the contractor complete it annually. For larger companies a separate executive level exercise driven by NIST 800-30, *Guide for Conducting Risk Assessments,* is more appropriate. This family also requires some form of vulnerability scanning and vulnerability management.

800-172 adds a whole lot to this – 7 enhancements.

> 3.11.1e Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and 818 recovery activities.

Before developing an SSP and designing security architectures and solutions, DoD contractors need to discuss what information they have, who would want that information, and what capabilities those threat actors may have.

> 3.11.2e Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.

The protective technologies prescribed in the original 110 controls – SIEM, IDPS, vulnerability scanning, etc. – are no longer enough. Contractors will need to actively search for toe holds and highly sophisticated streams of data exfiltration in their networks. Expect to implement SSL DPI and application layer gateways. Expect much tighter firewall requirements, especially on outbound traffic.

> 3.11.3e Employ advanced automation and analytics capabilities to predict and identify risks to organizations, systems, and system components.

This enhancement is intended to augment and/or supplement the required SOC and Incident Response capabilities that contractors will be required to have under 800-172. Vendors offering this kind of advanced Cyber Threat Intelligence services include FireEye and AlienVault.

> 3.11.4e Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.

This appears to mostly supplement and/or augment the other enhancements in 3.11, but there is some emphasis on external providers, which these days nearly every IT enterprise has. Contractors will need to not only list all of their providers by type (e.g., software as a service, platform as a service), but also document what security controls their external providers have in place.

3.11.5e Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.

The first version of 800-171 requires that the controls be reviewed on a regular basis, but how often was up to the contractor. 800-171B stated annually, so they seemed to have walked this back, making the enhancement kind of redundant. Maybe that will change again when they issue the final release.

3.11.6e Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.

3.11.7e Develop and update as required, a plan for managing supply chain risks associated with organizational systems and system components.

Contractors need to understand where they fall in the DoD supply chain and use that understanding in the development of their SSP and the selection of their security architecture. You may be making or handling what seem like mundane parts, but if those parts are critical to the operation of a nuclear sub or a B2 bomber, you are a target for reasons of Asymmetric Warfare.

3.12 Security Assessment

This family contains 4 basic requirements and no derived. The basic requirements are to:

- *Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.*
- *Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.*
- *Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.*
- *Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.*

These 4 controls taken together form the basic mandate to have a System Security Plan (SSP) and a Plan of Action and Milestones (POA&M). The SSP essentially authorizes the existence of and governs your IT security plan. The POA&M is a document that openly identifies unmet controls, along with a plan to remediate those unmet controls. Contractors are also required to treat the SSP as a living document that must be maintained.
800-172 adds a single enhancement here, but it is significant:

> 3.12.1e Conduct penetration testing [Assignment: organization-defined frequency], leveraging automated scanning tools and ad hoc tests using human experts.

While contractors are given some latitude on how these pen tests will be conducted – internal, external, white/gray/black box, Red Team, etc. – this is an entirely new requirement. Penetration Testing requires highly trained (and expensive) humans to execute properly. Penetration testing can vary wildly in scope, cost, and quality (this cannot be overstated), so the onus is completely on the buyer to find and engage with the right company.

3.13 System and Communications Protection

This family contains 2 basic requirements and 14 derived. The basic requirements are to:

- *Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.*

- *Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.*

All in, this family imposes a bunch of requirements – firewalls, network segmentation, DMZ's, FIPS encryption, session control, control of mobile code (Java, Flash) etc. Mostly standard stuff in a mature and well-designed IT environment. It does however require a "deny all, permit by exception" policy on **outbound** firewall traffic – something which in our experience most companies just don't do, or do it poorly.

800-172 adds 4 enhancements:

> 3.13.1e Create diversity in [Assignment: organization-defined system components] to reduce the extent of malicious code propagation.

At face value, this requirement seems scary – standardization of IT makes administration easier and more cost effective. The discussion of this control does say: "*Satisfying this requirement does not mean that organizations need to acquire and manage multiple versions of operating systems, applications, tools, and communication protocols……. For example, it is common for organizations to employ diverse anti-virus products at different parts of the infrastructure simply because each vendor may issue updates to new malicious code patterns at different times and frequency. Similarly, some organizations employ products from one vendor at the server level, and products from another vendor at the end-user level.*"

3.13.2e Disrupt the attack surface of organizational systems and system components.

Now we are getting into NSA type stuff. Meeting this control can be done (for example) by periodically changing IP schemes, DNS schemes, and network topologies. Extensive and creative use of virtualization is another means to achieve this sort of unpredictability and non-persistence.

3.13.3e Employ technical and procedural means to confuse and mislead adversaries.

Flat-out Information Warfare – use sandboxing, misdirection, and honeypots filled with deliberately tainted information.

3.13.4e Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.

Some options here in terms of logical isolation are data tagging, digital rights management (DRM), and data loss prevention (DLP) technology, or logical network segregation using VLAN's and ACL's.

Partial and/or total physical isolation is a good option as well – in large organizations with thousands of nodes, having a much smaller, separate network for handling CUI makes a lot of sense both in terms of cost and security.

3.14 System and Information Integrity

This family contains 3 basic requirements and 4 derived. The basic requirements are to:

- *Identify, report, and correct system flaws in a timely manner.*

- *Provide protection from malicious code at designated locations within organizational systems.*

- *Monitor system security alerts and advisories and take action in response.*

Contractors are expected to perform regular vulnerability scanning, have some kind of VMS (Vulnerability Management System) in place, anti-virus technology, and network and/or host-based intrusion detection – all standard protective technologies.

800-172 adds 6 enhancements:

> 3.14.1e Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.

Contractors will need to leverage UEFI, Secure Boot and TPM (Trusted Platform Modules). Cryptographic hashes and signatures will need to be verified as part of a formal configuration and change management process before new software and firmware is installed.

> 3.14.2e Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.

This is going to require some advanced integration between various protective technologies – having separate SIEM, IDPS, vulnerability scanning, etc. will not satisfy 800-172. Contractors will need an advanced UTM that integrates with A/V endpoint protection and DLP, all monitored from a dedicated SOC.

> 3.14.3e Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.

Contractors will need to ensure that PLC's (Programmable Logic Controllers), DCS (Distributed Control Systems), SCADA (Supervisory Control and Data Acquisition), embedded controllers, and all other IoT (Internet of Things) devices are properly isolated and/or protected. We often see massive cybersecurity blind spots in these systems, because contractors tend to be more focused on protecting their (mostly Windows based) business support systems.

> 3.14.4e Refresh [Assignment: organization-defined systems and system components] from a known, trusted state [Assignment: organization-defined frequency].

Using a verified trusted source, reload operating systems, applications and firmware on a regular basis to get rid of possible hidden APT toe holds.

> 3.14.5e Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI that is no longer needed.

Have formal policies and procedures in place to ensure that CUI is not retained longer than it is needed to support a specific program or project.

> 3.14.6e Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.

In addition to deploying highly integrated protective technologies and a dedicated SOC, contractors will need to participate in threat sharing consortia such as CERTCC, US-CERT, FIRST, ISAO, etc. Use this information in the security decision making process.

Conclusion

If NIST SP 800-171 revision 1 was a mid-sized family sedan, 800-172 would be an exotic sports car; much more complex and several times more expensive to both acquire and operate. For a very moderate sized, 25-50 endpoint system, The DoD is estimating some rather costly implementation figures:

- Process and IT configuration changes: $50K
- Network Isolation:
  - $100K to isolate existing network or existing network segment
  - $500K-2.5M to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $75K-150K (if not already met).

These estimates assume that affected contractors are already meeting the 110 controls in NIST 800-171r1, so they are in addition to those efforts. Out of the approximately 69,000 contractors currently processing CUI, around one half of one percent (345) would be subjected to the 33 enhancements of 800-172. While that may seem like a small number, based on our experience with the Defense Industrial Base, this figure is almost certain to rise.

About Appalachia Technologies

Appalachia Technologies is a leading Managed IT Services Provider in the Mid-Atlantic region. Founded in 2004, Appalachia has an established local presence in Central PA. Our roots are in technology infrastructure design, implementation, and management - with a heightened focus on cybersecurity. Appalachia is a **Top 50 Fastest Growing Company**, and a **Best Places to Work in PA.** For more information, visit us at**:** **https://appalachiatech.com/**

References

Security and Privacy Controls for Federal Information Systems and Organizations. (2015, January 22). Retrieved July 10, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (2018, July 06). Retrieved July 10, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Enhanced Security Requirements for Critical Programs and High Value Assets. (2019, June). Retrieved July 10, 2019, from https://csrc.nist.gov/CSRC/media/Publications/sp/800-171B/draft/documents/sp800-171B-draft-ipd.pdf

Enhanced Security Requirements for Protecting Controlled Unclassified Information A Supplement to NIST Special Publication 800-171. (2020, July). Retrieved October 27, 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172-draft.pdf

Request for Comments on Draft NIST Special Publication (SP) 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets. (n.d.). Retrieved July 10, 2019, from https://csrc.nist.gov/CSRC/media/Publications/sp/800-172/draft/documents/sp800-172-and-dod-cost-estimate-request-for-comments.pdf