At Implements of Honor we have twelve servers that are running the newest version of Microsoft Server. Each server has Active Directory, Domain Name System, Dynamic Host Configuration Protocol, Enterprise resource planning, research, and development network segment that we use for testing while keeping the actual environment safe, Microsoft Exchange Server that we use to send and receive emails, a filter for emails, and a cloud based secure web gateway. This gateway provides web security, data loss protection, a next-gen firewall, cloud application security, and advanced threat protection. We host our website on two Linux Apache servers. For our employees we have four hundred laptops with Windows 10, Microsoft 365 office applications, and other tools that we use to improve productivity in our company.

There are seven domains: users, workstations, LAN, WAN, LAN to WAN, remote access, and system/application. Employees will go into the user domain. The laptops they use will go into the workstation domain. The servers we use that run Microsoft Server belong in the LAN domain because the Microsoft Server is used for our internal network. The gateway that we use goes into the LAN to wan domain because the firewall on it protects our LAN from attacks that originate in the wan. The Linux servers go in the system/application domain. Users will connect to these servers through the WAN domain to access the company website.

Some general guidelines that Department of Defense (DoD) contractors should be following include classification of sensitive data, proper access controls, and keeping software and systems up to date. The DoD requires following NIST 800-171 guidelines. According to a blog written by Kevin Joyce found at netwrix.com and an article found at sysarc.com there are fourteen parts to the guidelines. These guidelines include monitor access in a system and only allow access to what employees need to do their jobs. Train employees in security and keep them aware of policies and how they relate to their jobs and inform them of internal and external

threats and how to respond. Keep track of data access and hold employees responsible for improper access. Use configurations to prevent access to unneeded systems and prevent installation of unauthorized software. Implement multi-factor authentication and strong password policies to ensure the person is who they say they are. Quickly find and respond to incidents and use intrusion detection systems and analyze what is happening on the network. Limit access to media with controlled unclassified information (CUI) and have proper destruction techniques for CUI or devices that hold CUI that are no longer needed. Limit access to controlled unclassified information (CUI) with physical controls in a building with things like cameras or locked doors. Track who accesses CUI and have plans for if employees who have accessed CUI leave the company. Regularly look for risks and complete testing to check for vulnerabilities in the system. Regularly look at the security of controls and policies in place and update those controls and policies as needed. Keep access points into systems secure and prevent communication of CUI and other important data over unsecured areas. Look for malicious code and keep software for security up to date.

DoD Contractors also need to follow CMMC policies. These include following NIST 800-171 guidelines. Improve based on a self-assessment score of NIST standards and submit score to DoD. Identify the scope of your organization. Another company should complete an optional first assessment. Implement changes in shortcomings of assessment. Choose a c3pao to complete the assessment and get certification once passed. Certification lasts 3 years.

One law that the DoD requires compliance with is DFARS 252.204-7012. It is also required to follow NIST 800-171 and become CMMC certified. Another law that is required to be followed is the Federal Information Security Management Act (FISMA) which is required when operating federal systems. The purpose of FISMA is to keep information safe and keep

systems safe. According to an article found at sysarc.com NIST 800-53 sets the guidelines required by FISMA.

NIST 800-53 is a framework that is continuously updated and provides standards that should be followed. This is a framework that is required for all federal systems as well. It is similar to NIST 800-171 in the things that it requires and the areas that it focuses on. It recommends location and classification of sensitive data and management of access control. NIST 800-53 is flexible.

Some unique things about NIST 800-53is the requirement of individual participation which includes consent and authorization. This framework also requires policies on social media restrictions so the data that is shared publicly is limited to safe information. There is also a requirement of contingency planning with disaster recovery sites.

Also, we should be following FAR 52.204-21. According to a source found at acquisition.gov FAR 52.204-21 includes limiting system access to authorized users. This involves limiting the tasks that users can complete. External connections should also have limits outside of the internal network and systems. Another thing to do is limit public information. Users or processes acting on behalf of users should be identified. Sanitize devices with sensitive Federal Contract Information when it is no longer needed. There should be systems and policies in place to monitor and log what a visitor accesses and does. Protect communications at external and internal boundaries. Public networks should be separate. Protect from malicious code and keep protections updated. Scan systems regularly to look for external files that could be dangerous.

Frameworks are an important part of cybersecurity. They help with risk management by setting guidelines on how to protect the several types of IT infrastructure. They help with

protecting all seven domains of IT infrastructure. Frameworks use best practices and are industry standard in organizations. There are different frameworks that work for different organizations based on their business and what laws they must follow.

The Department of Defense has developed a framework for risk management for their IT systems. This framework also applies to DoD contractors and is based on NIST publications. This framework provides roles and responsibilities. It also provides the steps required to fulfill risk management. The first step is to prepare by laying out the context of the business and the priority of security steps. The second step is categorizing the systems based on the information they hold and its importance. The third step is selecting the initial controls. The fourth step is to implement the controls and describe how they are used in the systems. The fifth step is to assess the effectiveness of the controls. The sixth step is to authorize controls if the risk that still exists is acceptable regarding the DoD and the country. A security plan document lays out the security that is being used. The seventh step is monitoring the controls, conducting assessments on risk, and creating reports on the effectiveness of the controls.

ISO 27001 is a framework that could be used to help protect the systems. This is a framework for Information Security Management. It will keep information secure, protect against attack, is a central framework, provides protection across the whole network, evolves for new security threats, costs less, protects integrity, confidentiality, and data availability.

The DoD has developed an architecture framework for their systems. Models are created to improve the architecture and managers' ability to complete tasks. There are models of data on the architecture that are created to visualize the architecture. CMMC 2.0 is a cybersecurity framework that is targeted towards government agencies and contractors with the government.

The DoD risk management framework applies to the IT infrastructure domains. An article found at dau.edu tells us that it requires everything to be kept secure and to have the correct configurations. The configurations we use need to be reviewed to ensure that they protect the network. ISO 27001 is another framework that should be used to set up a framework to protect devices in the organization.

Some policies that could apply to users include account creation and deletion for employees as they leave or join the company. Employees could be required to keep their passwords safe and not leave them out in the open and report any incident or access to documents that they should not be seeing. Policies for workstations could include how long they will stay unlocked without activity, how often they are patched, how often workstations are replaced.

LAN policies could include types of traffic that are allowed on the LAN. For strong security there could be a secure password requirement or a requirement for devices to prove that they are safe before they are allowed to access the LAN. One policy will be to keep the switches, routers, and other networking devices up to date to remove vulnerabilities. A good policy to have for LAN-to-WAN includes restricting traffic on both sides of the network to keep it secure.

According to an article found on LinkedIn there are many relevant policies to the domains. An article found on divyaaradhya.com also states some policies that are important for each domain.

Policies for the WAN include keeping the points where the data leaves the network. Do not send sensitive data over the WAN unless it is necessary for the business. Another WAN policy is keeping ports closed unless they are being used and do not open ports for unsecure protocols.

Policies for the Remote Access domain relate to connecting to devices or software while in a different location. Connections to the VPN need to remain secure and split tunneling is not allowed. Users only have a few attempts to connect to the VPN. If they fail their account will lock out. Passwords need to be strong. Another policy is keeping private data private. Do not show anyone around you information they shouldn't have access to.

Policies for the system/application domain apply to software used by the company. All software needs to be kept patched and secured. Files that are on the network will be scanned for viruses. Antivirus software that is updated with the most recent threats needs to be used.

According to an article by Brian Johnson on the website strongdm some good workstation standards include updating devices on a regular basis, for example every week or month, encrypting devices to prevent stealing of data, backing up on a regular basis, locking machines after 15 minutes of inactivity.

Microsoft has developed security baselines for Windows. Baselines are enforced when they will protect against unsecured means of changing settings or accessing data. Baselines are the basic settings that should be on all devices running Windows. This will protect the workstations for the company and stop users from doing things that put the company at harm with their company Windows 10 devices. These baselines are found online and should be used because they are safe. For the Windows Server there are good baseline security settings to follow. They are supposed to keep the server safe and are a good standard to have. There are steps to hardening servers that Windows has made that would be good to follow to keep the Windows server safe.

Standards for the LAN are limiting unsecure traffic types like HTTP, FTP, Telnet, etc. Another standard to follow is to keep networking devices safe by patching them every couple of

weeks and monitoring new vulnerabilities found. If there are known vulnerabilities, attempt to stop them from risking the security of the LAN.

A good standard to follow is to put a firewall outside the LAN and inside the LAN. This gives redundancies to increase the security of the network. A good standard would be to follow already published documentation. One example of that is NIST SP 800-12.

WAN domain standards include setting rules for the specific types of data that leave the network. This involves only allowing data from specific locations or with specific classifications to leave the network. If data has a high level of classification, it can't leave the network, if it needs to leave the network this needs approval to keep it safe. Data that leaves the network needs to be encrypted. All ports that are not actively used in the network must be closed. This includes any port that is used for protocols that transmit in plaintext. Ports that are secure still need to be closed unless they are being used to limit points for attackers to get into the network.

Remote Access domain standards include using a VPN service that does not allow split tunneling. Even if a user has a slow connection through a VPN a split-tunnel cannot be used because of the risks it causes. Account standards include locking out after 3 failed attempts. Passwords need to be at least ten characters long and they must include capital letters, special characters, and numbers. There are also standards of not accessing private data in a public place where someone could potentially see what you are looking at on your screen.

Standards for the system/application domain include checking once a week for updates to software used. Also, use settings to automatically update software to make sure it happens. All files will be scanned when they enter the network and users are not allowed to open suspicious files or click on suspicious links. Antivirus software needs to be updated with new vulnerabilities

every night to keep track of any new vulnerabilities that are discovered and protect systems as fast as possible.

Each domain in the IT infrastructure needs its own controls. Some controls that could go on the User domain are limiting access of data to what is needed for a user to do their job and requiring 2-factor authentication to log into accounts and workstations. Workstation domain controls could include adding software to protect the device from malware, using software that prevents adding files to the device, placing firewall controls on the device to prevent certain types of traffic. For the LAN domain controls could include firewall settings that prevent types of traffic from leaving the network or being sent across the network to other devices on the LAN. There could be firewall settings so that no one can connect to the LAN without an approved device that has the correct settings and patches on it. Use ACLs to stop traffic types that aren't safe. Some controls to use for the LAN to WAN include firewall controls that will stop sensitive data from being sent to the LAN. These firewall controls could include ACL's or using authentication to allow outside devices into the network. There could also be an IPS or IDS that finds suspicious activity and reports it and tries to stop it if it is an IPS.

Controls to use on the WAN domain include endpoints on the network having rules in place for what files can leave the network and having a way to check that the files are going to safe destinations. Use access control lists to verify that the files are sent to safe places through the WAN and nowhere else. According to a source found at passcamp.com the military uses AES-256 encryption so that is the encryption that will be used. According to winbuzzer.com Windows 10 has a way of closing ports on each computer and that will be used on the Windows devices to keep the ports from being used. There will also be port rules on routers and switches.

This provides redundancy which ensures that only necessary ports will be opened to keep the network safe.

Remote access domain controls include a VPN that can be set to only use a full tunnel and that uses a strong encryption method in transporting the data. Settings for accounts will be used to force the password requirements to be used. A control to keep others from seeing what is on a user's screen is to use a screen filter so the screen can only be seen by the user of the workstation.

Controls to use on the System/Application domain include scheduling the checking of updates and downloading those updates to happen daily. These can be scheduled with settings in operating systems or scripts. If this is not an option an IT employee will do this every day. Another control to include is using antivirus software to scan files that exist on the network. The software will alert of any suspicious files as soon as they are detected. The databases used to check for vulnerabilities will be updated every night so alerts can happen immediately and there is not a vulnerability that exists for many days on the network.

New employees will have to take security awareness training to understand the policies and their responsibility to follow the policies. This training will need to be renewed every year. Employees will be asked their opinions on the training and based on how well policies are followed changes will be made to the training to make it better.

Employees need to understand the importance of following these policies and a culture needs to be created to have following policies be normal.

The required frameworks will be implemented with the help of the legal department to ensure that all laws are being followed in the IT infrastructure and the frameworks the company

uses. The IT department will ensure that all changes happen correctly and audit systems regularly to ensure that the required controls are working correctly.

References

52.204-21 Basic Safeguarding of Covered Contractor Information Systems. 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. | Acquisition.GOV. (n.d.). Retrieved February 10, 2023, from https://www.acquisition.gov/far/52.204-21

Anonymous. (2018, July 2). *Server hardening standard (windows)*. IT Security. Retrieved March 2, 2023, from https://security.uconn.edu/server-hardening-standard-windows/

DFARS. 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. | Acquisition.GOV. (n.d.). Retrieved February 10, 2023, from https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Divya Aradhya. (2018, April 13). *Policies for the seven domains of a typical IT infrastructure*. Divya Aradhya. Retrieved March 24, 2023, from http://www.divyaaradhya.com/2018/03/13/policies-for-the-seven-domains-of-a-typical-it-infrastructure/

The DoDAF Architecture Framework Version 2.02. DODAF - DOD architecture framework version 2.02 - DOD deputy chief information officer. (n.d.). Retrieved March 2, 2023, from https://dodcio.defense.gov/library/dod-architecture-framework/

DOD INSTRUCTION 8510.01. (2022, July 19). Retrieved March 2, 2023, from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300

FISMA compliance: The Definitive Guide for Government Contractors. SysArc. (2019, February 4). Retrieved February 9, 2023, from https://www.sysarc.com/services/managed-security-services/fisma-compliance/

Hanna, K. T. (2022, December 13). *What is ISO 27001? – TechTarget definition*. WhatIs.com. Retrieved March 24, 2023, from https://www.techtarget.com/whatis/definition/ISO-27001

ISO/IEC 27001 and related standards - information security management. ISO/IEC 27001 and related standards. (2023, February 3). Retrieved March 1, 2023, from https://www.iso.org/isoiec-27001-information-security.html

Jackson, C. (2020, June 3). *Introducing the security configuration framework: A prioritized guide to hardening windows 10*. Microsoft Security Blog. Retrieved March 1, 2023, from https://www.microsoft.com/en-us/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/

Johnson, B. (2023, February 7). *Workstation security policy best practices*. StrongDM. Retrieved March 1, 2023, from https://www.strongdm.com/blog/workstation-security-policy

michalsons. (2023, January 5). The different types of policies. Retrieved March 1, 2023, from https://www.michalsons.com/focus-areas/information-technology-law/types-of-it-policies#:~:text=Categories%20of%20IT%20policies&text=Examples%20include%20an%20incident%20response,framework%20or%20data%20sharing%20policy.

Joyce, K. (2022, September 28). *DOD Cybersecurity Requirements: TIPS for compliance*. Netwrix Blog. Retrieved February 9, 2023, from https://blog.netwrix.com/2022/09/28/dod_cyber_security_requirements/

Kim, D., & Solomon, M. G. (n.d.). *Fundamentals of Information Systems Security, 4th Edition*. O'Reilly Online Learning. Retrieved February 8, 2023, from https://www.oreilly.com/library/view/fundamentals-of-information/9781284220742/xhtml/9781284220735_CH01_03.xhtml

Kittle, T. (2022, October 28). *Top cybersecurity requirements for government contractors*. Winvale Blog. Retrieved February 9, 2023, from https://info.winvale.com/blog/top-five-cybersecurity-requirements-for-government-contractors

Maskell, R. (2021, March 31). *How to open or close a port in Windows 10 firewall*. WinBuzzer. Retrieved March 23, 2023, from https://winbuzzer.com/2021/03/31/how-to-open-or-close-a-port-in-windows-10-firewall-xcxwbt/

Pabrai, U. A. (2022, January 25). *US DOD Launches Comprehensive CMMC 2.0 Cybersecurity Framework*. ISACA. Retrieved March 2, 2023, from https://www.isaca.org/resources/news-and-trends/industry-news/2022/us-dod-launches-comprehensive-cmmc-2-cybersecurity-framework

Risk Management Framework (RMF) for DoD Information Technology (IT). DAU. (n.d.). Retrieved March 24, 2023, from https://www.dau.edu/acquipedia/pages/articledetails.aspx#!245

Scarfone, K., Jansen, W., & Tracy, M. (2008, July). *Guide to general server security - NIST*. NIST Special Publication 800-123. Retrieved March 2, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

Tierney, M. (2022, January 13). NIST 800-53: A Guide to Compliance. Retrieved February 10, 2023, from https://blog.netwrix.com/2021/03/03/nist-800-

53/#:~:text=NIST%20800%2D53%20is%20mandatory,with%20sensitive%20or%20regulated%20data

Vinaypamnani-Msft. (2023, February 17). *Security Baselines Guide*. guide | Microsoft Learn. Retrieved March 1, 2023, from https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

Wand, D. (2020, June 30). *Securing the seven domains of IT infrastructure*. LinkedIn. Retrieved March 23, 2023, from https://www.linkedin.com/pulse/securing-seven-domains-infrastructure-dan-wand/

What is military-grade encryption? PassCamp. (2022, April 7). Retrieved March 23, 2023, from https://www.passcamp.com/blog/what-is-military-grade-encryption/#:~:text=Military%2Dgrade%20encryption%20refers%20to%20AES%2D256.&text=This%20encryption%20method%20was%20established,that%20utilizes%20256%2Dbit%20keys.