**Recommendations**

1. **Family:** Access Control  
 **Enhanced Security Requirements:** "Employ dual authorization to execute critical or sensitive system and organizational operations."  
 **Level of Compliance:** Not begun  
 **Recommendation:** To achieve compliance, the organization should establish and implement policies and procedures for dual authorization, which include defining what constitutes a critical or sensitive operation, identifying the individuals authorized to perform dual authorization, and outlining the process for executing dual authorization. The organization should also provide training to personnel on the dual authorization process and the importance of following it to maintain the security of the system and organization.

2. **Family:** Configuration Management  
 **Enhanced Security Requirements:** Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.  
 **Level of Compliance:** Not begun

**Recommendation:**  
To better prepare for compliance with CMMC (Cybersecurity Maturity Model Certification) Level 3's enhanced security requirement for Configuration Management, the organization should establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components. This may involve developing a documented process for component approval and implementing a secure repository to store approved components. The organization should also ensure that all personnel involved in the configuration management process are trained on the new process and are aware of their responsibilities to ensure compliance. Additionally, the organization should regularly review and update the repository to ensure it remains up-to-date and accurate.

3. **Family:** Incident Response  
 **Enhanced Security Requirements:** Establish and maintain a security operations centre capability that operates [Assignment: organization-defined time period].  
 **Level of Compliance:** Not begun

**Recommendation:**  
 It is important for the organization to define the time for the security operations centre capability to operate and ensure that it is maintained and operational during that time. The security operations centre should be equipped to detect, analyse, and respond to security incidents and have appropriate resources and tools available. It is recommended that the organization regularly test and evaluate the effectiveness of their security operations centre capability to ensure that it is functioning as intended.

4. **Family:** Incident Response  
 **Enhanced Security Requirements:** Establish and maintain a security operations centre capability that operates [Assignment: organization-defined time period].  
 **Level of Compliance:** Not begun

**Recommendation:**  
 The organization should establish and maintain a cyber incident response team that can be deployed within the organization-defined period. This may include:

* Developing a documented plan for incident response that includes the roles and responsibilities of the cyber incident response team.
* Identifying and training personnel who will serve as members of the cyber incident response team.
* Conducting regular drills and exercises to ensure that the team is prepared to respond effectively to cyber incidents.
* Ensuring that the team has access to the necessary resources, including technology, tools, and information, to respond to cyber incidents.
* Establishing communication protocols to ensure that the team can effectively communicate with key stakeholders during an incident.

5. **Family:** Risk Assessment  
 **Enhanced Security Requirements:** 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 recovery activities.  
 **Level of Compliance:** Not begun  
 **Recommendation:**  
 It is recommended to identify and select appropriate sources of threat intelligence that can guide and inform their risk assessment process. The organization should develop a plan to integrate the threat intelligence into their risk assessment process and ensure that it is consistently updated to remain relevant. The organization should also ensure that the threat intelligence is used to inform the development of their systems and security architectures, the selection of security solutions, and their monitoring, threat hunting, response, and recovery activities. Additionally, the organization should ensure that they have a process in place for reviewing and updating their threat intelligence sources on a regular basis to ensure that the information remains current and relevant.

6. **Family:** Risk Assessment **Enhanced Security Requirements:** 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.  
 **Level of Compliance:** Not begun **Recommendation:** The organization should establish a plan and timeline for implementing this requirement, including defining the frequency of these activities and the specific systems to be included in the threat hunting process. The organization can also consider investing in appropriate tools and technologies to support effective cyber threat hunting activities.

7. **Family:** Risk Assessment **Enhanced Security Requirements:** Assess, respond to, and monitor supply chain risks associated with organizational systems and system components. **Level of Compliance:** Not begun  
 **Recommendation:** Organization shouldidentify potential risks in the supply chain and taking appropriate measures to mitigate them, such as vetting suppliers and monitoring their security practices. It is important to begin implementing this requirement as soon as possible to ensure compliance with CMMC Level 3 and to protect the organization from potential supply chain attacks.  
8. **Family:** Risk Assessment **Enhanced Security Requirements:** Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [Assignment: organization-defined frequency]. **Level of Compliance:** Not begun  
 **Recommendation:** The plan should be updated regularly as determined by the organization to ensure that it remains relevant and effective in mitigating supply chain risks. The organization should also ensure that the plan addresses all relevant supply chain risk factors and is integrated into the organization's overall risk management framework. This can be achieved by conducting a thorough risk assessment of the organization's supply chain and identifying the specific risks that need to be managed. The organization should also ensure that all relevant stakeholders are involved in the process, including suppliers and customers, to ensure that the plan is comprehensive and effective.

9. **Family:** Security Assessment **Enhanced Security Requirements:** Conduct penetration testing [Assignment: organization-defined frequency], leveraging automated scanning tools and ad hoc tests using subject matter experts.

**Level of Compliance:** Not begun  
**Recommendation:** The organization should develop a plan for conducting regular penetration testing at an organization-defined frequency. The plan should include the use of automated scanning tools and ad hoc tests by subject matter experts. The organization should also ensure that the individuals conducting the tests are qualified and knowledgeable in the latest security testing techniques. It is important for the organization to keep records of the results of the penetration testing, including any vulnerabilities found and the actions taken to remediate them. The organization should also review and update their security plan based on the results of the testing to ensure that their systems and networks are adequately protected.

10. **Family:** Security & Communications Protection **Enhanced Security Requirements:** Employ [Assignment: organization-defined technical and procedural means] to confuse and mislead adversaries. **Level of Compliance:** Not begun  
 **Recommendation:** To comply with this requirement, the organization may consider implementing deception technologies such as honeypots, honeynets, and honeytokens to create a false impression of the network and confuse attackers. Additionally, the organization can also implement procedures such as regularly changing login credentials and limiting access privileges to reduce the likelihood of successful attacks. It is important to note that implementing deception technologies and procedures can be complex and may require specialized knowledge and expertise.

11. **Family:** System & Information integrity  
 **Enhanced Security Requirements:** Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI (Controlled Unclassified Information) that is no longer needed.  
 **Level of Compliance:** Not begun  
 **Recommendation:**  
To begin implementing this requirement, the organization should conduct a thorough risk assessment to identify potential adversaries and the tactics they may use to gain access to sensitive information. Once identified, the organization should implement technical controls such as intrusion detection and prevention systems, access controls, and encryption to protect against unauthorized access. In addition to technical controls, the organization should also implement procedural controls such as training employees on security awareness, incident response procedures, and regular security assessments to ensure that security measures are effective and up to date.

12. **Family:** System & Information integrity  
 **Enhanced Security Requirements:** Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.  
 **Level of Compliance:** Not begun  
 **Recommendation:**  
 The organization should start implementing the enhancement related to using threat indicator information and effective mitigations obtained from external organizations to guide and inform intrusion detection and threat hunting. This may involve identifying and establishing relationships with relevant external organizations and implementing processes to regularly receive and utilize threat indicator information and effective mitigations. The organization should also consider establishing dedicated team or personnel responsible for intrusion detection and threat hunting activities.  
  
  
  
  
**Partially Implemented:**

* **Family:** Access Control.
* **Enhanced Security Requirements:**  Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.
* **Level of Compliance:** Partially implemented.
* **Recommendation:**

1. Identify the security domains and information flows: The organization should conduct a thorough assessment to identify the security domains and information flows between connected systems. This assessment will help the organization to determine which information transfer solutions are required to control the information flows between the security domains.
2. Select appropriate secure information transfer solutions: Based on the assessment, the organization should select appropriate secure information transfer solutions that meet the organization's needs and comply with CMMC Level 3 requirements. These solutions may include virtual private networks (VPNs), firewalls, intrusion detection and prevention systems, and other security controls.
3. Configure and test secure information transfer solutions: The organization should configure and test the selected secure information transfer solutions to ensure that they are properly installed, configured, and functioning as intended. The organization should also ensure that the solutions comply with CMMC Level 3 requirements.
4. Develop and implement policies and procedures: The organization should develop and implement policies and procedures that govern the use of the secure information transfer solutions. These policies and procedures should cover access controls, data protection, incident response, and other areas relevant to information transfer security.
5. Train personnel: The organization should provide training to personnel who will be using the secure information transfer solutions. This training should cover the policies and procedures, as well as best practices for using the solutions securely.

**Family:** Identification and Authentication.

**Enhanced Security Requirements:** 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.

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Identify systems and components that require password management: The organization should conduct an inventory of all systems and components that require password management and identify which ones do not support multifactor authentication or complex account management.
2. Select a password management solution: The organization should select a password management solution that meets CMMC Level 3 requirements and the organization's needs. The solution should support 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.
3. Implement the password management solution: The organization should implement the selected password management solution, configure it according to CMMC Level 3 requirements, and test it to ensure that it is functioning as intended.
4. Train personnel: The organization should provide training to personnel who will be using the password management solution. This training should cover how to generate and manage passwords, as well as how to use the password management solution securely.
5. Develop and implement policies and procedures: The organization should develop and implement policies and procedures that govern the use of the password management solution. These policies and procedures should cover access controls, data protection, incident response, and other areas relevant to password management.

**Family:** Identification and Authentication.

**Enhanced Security Requirements:** 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.

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Inventory system components: The organization should conduct an inventory of all system components that connect to organizational systems. This inventory should include hardware devices, software applications, and any other components that may connect to the network.
2. Develop trust profiles: The organization should develop trust profiles for each system component based on their level of risk. A trust profile is a set of security controls and configurations that must be met for a system component to connect to the network.
3. Configure security controls: The organization should configure security controls on all system components based on their trust profile. These controls may include authentication mechanisms, encryption, access controls, and other security measures.
4. Implement automated or manual/procedural mechanisms: The organization should implement 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 may involve deploying network access control (NAC) solutions, firewalls, intrusion detection/prevention systems, or other security tools.
5. Train personnel: The organization should provide training to personnel who will be using the automated or manual/procedural mechanisms. This training should cover how to identify and authenticate system components, as well as how to use the security controls and configurations.

**Family:** Risk Assessment

**Enhanced Security Requirements:** Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Conduct a comprehensive review of existing automation and analytics capabilities to identify gaps in support of analysts to predict and identify risks to the organization, systems, and system components.
2. Develop a roadmap to enhance automation and analytics capabilities to address identified gaps and meet the enhanced security requirements of CMMC Level 3.
3. Implement additional automated tools and technologies such as machine learning, artificial intelligence, and advanced analytics to support analysts in predicting and identifying risks.
4. Establish clear processes and procedures for integrating automated tools and technologies into the risk assessment process, including training for personnel responsible for using these tools.
5. Conduct regular assessments to ensure that the automated tools and technologies are functioning effectively and efficiently and that they are providing the necessary support to analysts.

**Family:** Risk Assessment

**Enhanced Security Requirements:** 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.

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Define the frequency at which security solutions will be assessed and evaluated for effectiveness based on current and accumulated threat intelligence.
2. Conduct a comprehensive review of existing security solutions to identify gaps and areas of improvement in addressing anticipated risk to organizational systems and the organization.
3. Develop a risk assessment plan that incorporates the defined frequency of security solution assessment and evaluation, including a schedule of assessments and criteria for evaluating effectiveness.
4. Incorporate current and accumulated threat intelligence into the risk assessment process to identify potential threats and vulnerabilities that may impact the effectiveness of security solutions.
5. Establish clear processes and procedures for conducting assessments and evaluations, including the roles and responsibilities of personnel responsible for conducting assessments, reporting results, and implementing improvements.

**Family:** System and Communications Protection.

**Enhanced Security Requirements:** Create diversity in [Assignment: organization-defined system components] to reduce the extent of malicious code propagation.

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Determine which system components will be included in the diversity effort based on risk assessment and other relevant factors.
2. Develop a plan to create diversity in the identified system components, including a timeline, roles and responsibilities, and specific steps for implementation.
3. Utilize different hardware, software, and firmware components to increase diversity, which will reduce the extent of malicious code propagation.
4. Implement strict configuration management procedures to ensure that all components are properly configured and maintained.
5. Regularly review and update the diversity plan to ensure that it remains effective and up to date with changing threats and technologies.

**Family:** System and Communications Protection.

**Enhanced Security Requirements: I**mplement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [Assignment: organization-defined changes and frequency of changes by system and system component].

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Conduct a risk assessment to identify which systems and components are critical to the organization and require the implementation of changes to introduce a degree of unpredictability.
2. Identify and document the specific changes to be implemented, including the frequency of changes and which systems and components they will apply to.
3. Develop a plan to implement the changes, including timelines, roles and responsibilities, and a method for testing the changes to ensure they are effective.
4. Ensure that changes are implemented in a way that does not negatively impact system performance or availability.
5. Consider implementing changes in a phased approach to reduce the impact on operations and to allow for testing and evaluation of each change.

**Family:** System and Information Integrity.

**Enhanced Security Requirements:** 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.

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Review the list of organization-defined systems and components to determine whether they should be included in the scope of the specified enhanced security requirements or segregated in purpose-specific networks.
2. Develop a clear and concise policy that outlines the scope of the specified enhanced security requirements and the requirements for segregating purpose-specific networks.
3. Ensure that all relevant staff members receive adequate training on the organization's policy regarding the inclusion of systems and components in the scope of the specified enhanced security requirements.
4. Regularly monitor and audit systems and components to ensure that they are in compliance with the specified enhanced security requirements or are segregated in purpose-specific networks.
5. Conduct periodic risk assessments to identify and evaluate any potential risks associated with the specified enhanced security requirements or the segregation of purpose-specific networks, and take appropriate steps to address these risks.

**Family:** System and Information Integrity.

**Enhanced Security Requirements:** Refresh [Assignment: organization-defined systems and system components] from a known, trusted state [Assignment: organization-defined frequency].

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Conduct a thorough review of the organization-defined secure information transfer solutions and select a solution that meets the CMMC Level 3 requirements. Ensure that the solution provides adequate control over information flows between security domains on connected systems. Once a solution is selected, ensure that it is fully implemented and that all relevant personnel are trained on its proper use.
2. Develop and implement a comprehensive password management program that includes automated mechanisms for password generation, protection, rotation, and management for systems and system components that do not support multifactor authentication or complex account management. Ensure that all personnel are trained on the proper use of the program.
3. Implement an automated or manual/procedural mechanism 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. Ensure that all relevant personnel are trained on the proper use of the mechanism.
4. Develop and implement a comprehensive risk management program that includes advanced automation and analytics capabilities to support analysts in predicting and identifying risks to organizations, systems, and system components. Ensure that all relevant personnel are trained on the proper use of the program.
5. Assess the effectiveness of security solutions on a regular basis to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence. Develop a schedule for the assessments and ensure that all relevant personnel are aware of the schedule and the assessment process.

**Family:** System and Information Integrity.

**Enhanced Security Requirements:** Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques].

**Level of Compliance:** Partially implemented.

**Recommendation:**

1. Identify the specific systems and components that fall under the scope of the enhanced security requirements and ensure that they are fully included in the compliance efforts.
2. Develop a plan and schedule for refreshing the systems and components from a known, trusted state, ensuring that the frequency of refreshes meets the organization's needs.
3. Determine the appropriate verification methods or techniques for the identified security-critical software, firmware, and hardware components and implement them as soon as possible. It may be helpful to consult with subject matter experts or vendors to ensure the methods and techniques are effective.
4. Monitor the effectiveness of the implemented controls and make any necessary adjustments to ensure compliance with the CMMC Level 3 requirements.