GUIDE

Redspin
A Division of Clearwater

Preparing for Your CMMC Interview: Commonly Asked Questions – System and Communications Protection Edition

This domain emphasizes the safeguarding of information as it is transmitted across networks and systems, ultimately ensuring that messages and/or data sent and received can remain confidential and unaltered. This may include measures such as encryption, firewalls, intrusion detection systems (IDSs), secure communication protocols, and more, ultimately securing this data from external threats.

TABLE OF CONTENTS

Key

Domain Family

Identifier

Basic | Derived

Security Requirement

Security Requirement Table of Contents

System and Communications Protection

- Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).....5
- Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.....6
- Control and monitor the use of mobile code.....7
- Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29]. 8
- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.....9
- Establish and manage cryptographic keys for cryptography employed in organizational systems.....10
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.....11
- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).....12
- Protect the authenticity of communications sessions.....14
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.....15
- Prevent unauthorized and unintended information transfer via shared system resources.....16
- Separate user functionality from system management functionality.....17
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.....19
- 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.....20
- Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.....21
- Protect the confidentiality of CUI at rest.....22

As you prepare for your organization's assessment, it's important to understand what to expect during the interview process. Individuals can anticipate a range of questions that will be both comprehensive and reflective of several key areas intended to assure that the controls are implemented correctly and performing as expected. Interview sessions typically follow a basic pattern to help inform this decision. Below is an example interview session construct. Though not all inclusive these guides provide typical questions asked during an assessment.

Typical Question Format:

Policy and Procedures:

- How does your organization's security policy address the encryption of Controlled Unclassified Information (CUI) on mobile devices and platforms?
- Can you provide documentation or guidelines that mandate encryption on mobile devices and platforms when handling CUI?

Implementation:

- What encryption standards or protocols does your organization use for CUI on mobile devices?
- Are there specific mobile device management (MDM) or mobile application management (MAM) tools in place to enforce encryption on mobile devices and platforms?
- How do you ensure that all mobile devices used within the organization have encryption enabled?

Monitoring and Auditing:

- How do you monitor and verify that CUI remains encrypted on mobile devices and platforms?
- Are there any auditing mechanisms in place to check for devices that might have encryption disabled or bypassed?
- Can you provide recent audit logs or reports showing encryption checks for mobile devices?

Incident Handling:

- Have there been any incidents where CUI was found unencrypted on a mobile device? If so, how was it handled?
- What are the consequences or actions taken against users who fail to encrypt CUI on their mobile devices?

Training and Awareness:

- How are employees made aware of the importance of encrypting CUI on mobile devices?
- Is there a specific training module or awareness campaign focused on mobile device encryption?

Technical:

- Can you demonstrate the encryption settings on a sample mobile device used within the organization?
- Are there any exceptions or scenarios where CUI might not be encrypted on mobile devices, and how are these exceptions handled?

Third-party and BYOD:

- How does your organization ensure that third-party vendors or contractors adhere to this encryption requirement when accessing CUI on mobile devices?
- If you have a Bring Your Own Device (BYOD) policy, how do you ensure that personal devices encrypt CUI?

System and Communications Protection

SC.L2-3.13.7

Derived

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

- How does your organization address the risk of split tunneling in its remote access policies?
- What mechanisms or tools are in place to detect and prevent remote devices from establishing split tunnels?
- How do you ensure that remote devices connected to your organizational systems don't simultaneously communicate with external networks?
- What monitoring solutions are employed to oversee remote device connections and ensure compliance with the no-split-tunneling policy?
- Are users educated or trained about the risks and prohibitions associated with split tunneling?
- How do you handle violations or attempts to bypass the split tunneling prevention mechanisms?
- How do you manage exceptions or scenarios where split tunneling might be required for specific business purposes?
- Describe any challenges or issues you've faced related to preventing split tunneling and how they were addressed.
- How do you ensure third-party or partner devices connecting to your systems adhere to the no-split-tunneling policy?
- Are there automated alerts or notifications set up to detect potential split tunneling activities?
- How do you test or validate the effectiveness of mechanisms in place to prevent split tunneling?
- How do you handle software or applications on remote devices that might inherently use split tunneling features?
- What processes are in place to review and update the split tunneling prevention mechanisms in light of evolving threats or technologies?
- Are there periodic security audits or assessments to validate adherence to the no-split-tunneling policy and its effectiveness?
- How do you manage user feedback or concerns related to the restriction of split tunneling?
- How do you ensure continuity of operations and user experience while enforcing the no-split-tunneling policy?
- How do you integrate split tunneling prevention with other security measures or VPN configurations?

- How do you stay informed about industry best practices or emerging threats related to split tunneling?
- In scenarios of remote global access, how do you handle split tunneling considerations given varying network conditions or requirements?
- How do you ensure that the approach to preventing split tunneling aligns with NIST guidelines and the organization's broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.14

Derived

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

- How does your organization implement security controls for VoIP technologies?
- What tools or platforms are used to monitor VoIP traffic and usage within your environment?
- How do you ensure encryption and secure protocols are in place for VoIP communications?
- Are there specific policies or guidelines provided to employees regarding the secure use of VoIP technologies?
- How do you handle authentication and access control for VoIP systems and endpoints?
- What measures are in place to detect and prevent unauthorized or malicious VoIP traffic?
- How do you segregate or isolate VoIP traffic from other network traffic to ensure its security?
- How frequently are VoIP security configurations and controls reviewed and updated?
- How do you manage and secure VoIP endpoints, such as phones, softphones, or VoIP applications?
- Are there automated alerts or mechanisms in place to detect anomalies or potential security incidents related to VoIP?
- Describe any challenges or issues you've faced related to VoIP security and how they were addressed.
- How do you ensure third-party VoIP solutions or services used by your organization adhere to security best practices?
- How do you handle data retention, backup, and recovery for VoIP systems and communications?
- How do you educate and train users about potential risks and best practices related to VoIP usage?
- How do you manage patches, updates, or vulnerabilities associated with VoIP software or hardware?
- How do you ensure continuity and availability of VoIP services while maintaining security?
- Are there specific protocols or controls for VoIP communications that involve sensitive or confidential information?

- How do you integrate VoIP security monitoring with other security tools or incident response systems?
- Are there periodic security audits or assessments specific to VoIP technologies and their usage?
- How do you ensure that the approach to controlling and monitoring VoIP aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.13

Derived

Control and monitor the use of mobile code.

- How does your organization define mobile code in the context of its systems and operations?
- What policies and procedures are in place for the use of mobile code?
- How do you ensure that only authorized mobile code runs on organizational systems?
- Describe the tools or mechanisms used to monitor the execution of mobile code.
- How do you verify the authenticity and integrity of mobile code before it's executed?
- Are there specific repositories or sources from which mobile code is approved or allowed?
- How do you handle exceptions or requests to use mobile code that falls outside of established policies?
- How do you educate users about the risks and policies associated with mobile code?
- Are there automated alerts or mechanisms in place to detect unauthorized mobile code execution?
- How do you integrate mobile code monitoring with other security systems or protocols?
- What measures are in place to prevent or mitigate mobile code from exploiting vulnerabilities in organizational systems?
- How frequently is the list of authorized mobile code sources or repositories reviewed and updated?
- Describe any challenges or issues you've encountered related to mobile code and how they were addressed.
- How do you handle updates or patches to mobile code to ensure they don't introduce security risks?
- How do you ensure third-party vendors or integrated solutions adhere to your organization's mobile code policies?
- How do you manage mobile code in cloud environments or remote access scenarios?
- Are there specific controls or restrictions for mobile code on critical or high-security systems?
- How do you stay updated on best practices and industry standards related to mobile code security?

- Are there periodic security audits or assessments to validate the control and monitoring of mobile code?
- How do you ensure that the approach to controlling and monitoring mobile code aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.12

Derived

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].

- How do you ensure that collaborative computing devices cannot be remotely activated without proper authorization?
- What mechanisms or features are in place to provide clear indications to users when collaborative computing devices are in use?
- How do you handle exceptions or approved scenarios where remote activation is necessary?
- Describe the tools or platforms used to monitor and manage remote access to collaborative computing devices.
- Are there automated alerts or mechanisms in place to detect unauthorized remote activation attempts?
- How do you educate users about the indications of device usage and the risks associated with unauthorized remote activation?
- What measures are in place to protect against potential attacks or unauthorized access to collaborative computing devices?
- How frequently are the configurations and settings related to this practice reviewed and updated?
- How do you handle third-party or external devices that might be integrated into your collaborative computing environment?
- How do you ensure that software or firmware updates to collaborative computing devices don't inadvertently alter the security settings related to remote activation?
- Describe any challenges or issues you've faced related to remote activation of devices and how they were addressed.
- How do you test or validate the effectiveness of mechanisms that indicate device usage to users present at the device?
- How do you manage and track user feedback or concerns related to this practice?
- Are there specific protocols or measures in place for high-security environments or sensitive meetings?
- How do you integrate this practice with other security protocols, especially those related to remote access or device management?

- How do you handle older or legacy collaborative computing devices in the context of this practice?
- Are there periodic security audits or assessments to validate the effective enforcement of this practice?
- How do you stay updated on industry best practices or threats related to remote activation of collaborative computing devices?
- In the event of a breach or unauthorized remote activation, what response protocols are in place?
- How do you ensure that the approach to managing remote activation and device usage indications aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.11

Derived

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

- Which cryptographic modules are you currently using to protect the confidentiality of CUI?
- Are these cryptographic modules FIPS 140-2 or FIPS 140-3 validated?
- Can you provide documentation or certification numbers for the FIPS-validated cryptographic modules in use?
- How do you ensure that only FIPS-validated cryptographic methods are employed across all relevant systems and applications?
- How frequently do you review and update cryptographic methods to ensure they align with the latest FIPS standards?
- What processes are in place to handle situations where FIPS validation may be compromised or outdated due to vulnerabilities or advancements in cryptographic attacks?
- How do you train and educate relevant personnel about the importance of using FIPS-validated cryptography for CUI?
- Are there any exceptions or scenarios where non-FIPS validated cryptography is used, and if so, how are they justified and managed?
- How do you ensure third-party vendors, solutions, or integrated systems adhere to FIPS-validated cryptographic standards when handling CUI?
- How do you monitor and verify the correct implementation of FIPS-validated cryptographic modules in real-time operations?
- How do you handle cryptographic key management, generation, storage, and destruction in line with FIPS requirements?

- Are there automated alerts or mechanisms to detect any deviations from FIPS-validated cryptographic standards?
- How do you integrate FIPS-validated cryptography enforcement with other security tools or protocols?
- Describe any challenges or issues you've encountered in implementing or maintaining FIPS-validated cryptography and how they were addressed.
- How do you stay updated on changes or updates to FIPS cryptographic standards?
- How do you test or validate the effectiveness and correct implementation of FIPS-validated cryptographic modules?
- Are there periodic security audits or assessments to verify adherence to FIPS-validated cryptographic practices?
- How do you ensure backup and recovery processes also adhere to FIPS-validated cryptographic standards when dealing with CUI?
- In cases where CUI is transferred or shared externally, how do you ensure the data remains protected with FIPS-validated cryptography?
- How do you ensure that the approach to using FIPS-validated cryptography aligns with the broader NIST guidelines and cybersecurity objectives of the organization?

System and Communications Protection

SC.L2-3.13.10

Derived

Establish and manage cryptographic keys for cryptography employed in organizational systems.

- Describe your organization's process for generating cryptographic keys.
- How do you store and protect private and secret cryptographic keys?
- What mechanisms are in place to ensure the secure distribution and transmission of cryptographic keys?
- How do you handle the lifecycle management of cryptographic keys, including generation, distribution, rotation, and retirement?
- What tools or platforms do you use for cryptographic key management?
- Are there automated alerts or mechanisms in place to detect potential unauthorized access or misuse of cryptographic keys?
- How frequently do you rotate or change cryptographic keys?
- Describe the process for revoking or invalidating cryptographic keys when needed.
- How do you ensure redundancy and backup of critical cryptographic keys?

- What measures are in place to protect cryptographic keys during transit and at rest?
- How do you manage and monitor third-party access to cryptographic keys?
- Describe any hardware security modules (HSMs) or dedicated key management solutions employed.
- How do you handle cryptographic key management for cloud services or external platforms?
- Describe the process for recovering from the loss or compromise of a cryptographic key.
- How do you ensure compliance with industry standards or best practices related to cryptographic key lengths and algorithms?
- How are personnel trained and made aware of their responsibilities related to cryptographic key management?
- Are there periodic security audits or assessments to validate the security and integrity of your cryptographic key management practices?
- How do you address feedback or concerns related to cryptographic key management?
- Describe any challenges or issues you've faced related to cryptographic key management and how they were addressed.
- How do you ensure that your approach to cryptographic key management aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.9

Derived

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

- How does your organization define the criteria for terminating inactive network connections?
- What mechanisms or tools are in place to automatically terminate communications sessions after a set period of inactivity?
- How do you determine the appropriate duration of inactivity before a session is terminated?
- Are there exceptions or specific scenarios where the inactivity threshold might be extended or shortened?
- Describe the processes used to inform users about session termination due to inactivity.
- How do you ensure that the termination of connections doesn't result in data loss or disrupt ongoing operations?
- What protocols are in place for users to re-establish a terminated session safely and securely?
- How do you handle sessions that require prolonged connectivity or are critical in nature?

- Are there automated alerts or mechanisms in place to detect and respond to sessions that bypass the termination criteria?
- How do you integrate session termination with other security measures, such as user authentication or session encryption?
- How do you handle third-party or external connections in terms of session termination due to inactivity?
- Are there different thresholds or protocols for session termination on different types of systems or applications within the organization?
- Describe any challenges or issues you've encountered related to session termination and how they were addressed.
- How do you educate and train users about the importance of session termination and the risks of prolonged inactivity?
- How do you test or validate the effectiveness of your session termination mechanisms?
- How do you manage feedback or concerns from users or departments about session termination protocols?
- How do you stay updated on best practices and industry standards related to session termination and inactivity thresholds?
- Are there periodic security audits or assessments to verify the consistent application of session termination protocols across all systems?
- How do you ensure that the session termination process doesn't inadvertently introduce new vulnerabilities or attack vectors?
- How do you ensure that the approach to terminating network connections due to inactivity aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.6

Derived

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

- How does your organization implement the "deny all, permit by exception" principle for network communications?
- What tools or solutions do you use to enforce this network traffic policy?
- How do you determine which network communications are exceptions and should be permitted?
- Describe the process for requesting and approving exceptions to the default deny policy.
- How frequently are the permitted exceptions reviewed and validated?

- How do you ensure that unauthorized or unexpected network traffic is promptly detected and addressed?
- How do you handle emergency or urgent needs that might require temporary changes to the network traffic policy?
- What measures are in place to educate and inform stakeholders about the "deny all, permit by exception" principle?
- How do you manage third-party or external connections in light of this network traffic policy?
- Are there specific protocols or considerations for managing network traffic in cloud environments or remote access scenarios?
- How do you test or validate the effectiveness of the "deny all, permit by exception" policy in preventing unauthorized network communications?
- Describe any challenges or issues you've faced in implementing this network traffic policy and how they were addressed.
- How do you integrate the enforcement of this policy with other security tools or incident response systems?
- How do you ensure that the "deny all, permit by exception" approach doesn't inadvertently hamper critical business processes or functions?
- Are there automated alerts or mechanisms in place to notify relevant personnel of denied network communication attempts?
- How do you handle feedback or concerns from departments or users about network communication restrictions?
- How do you collaborate with external entities, industry peers, or security experts to enhance your approach to network traffic management?
- Are there periodic audits or assessments to validate the effectiveness and appropriateness of the network traffic exceptions in place?
- How do you ensure continuity in network access and communication during system updates, migrations, or the introduction of new technologies?
- How do you ensure that the approach to network traffic management aligns with the organization's broader cybersecurity objectives and NIST compliance requirements?

System and Communications Protection

SC.L2-3.13.15

Derived

Protect the authenticity of communications sessions.

- What mechanisms do you employ to ensure the authenticity of communications sessions?
- How do you implement and manage digital signatures or certificates to authenticate communication sessions?
- Describe the protocols and tools in place to prevent man-in-the-middle attacks.
- How do you ensure the authenticity of remote communication sessions, especially those originating from external networks?
- What methods are used to validate the identity of devices or systems involved in a communication session?
- How do you handle communications that fail authenticity checks?
- Describe the process for issuing, renewing, and revoking authentication credentials or certificates.
- How do you ensure secure handshakes between communicating devices or systems?
- Are there automated alerts or mechanisms to detect potential breaches in communication authenticity?
- How do you manage and monitor third-party or partner communication sessions to ensure their authenticity?
- How do you integrate communication session authenticity with other security controls like encryption or intrusion detection?
- How frequently do you review and update your methods and tools for ensuring communication authenticity?
- How do you ensure that communication authenticity mechanisms don't hinder performance or user experience?
- What training or awareness programs are in place to educate users about the importance of communication session authenticity?
- How do you handle legacy systems or older communication protocols in terms of ensuring session authenticity?
- Describe any challenges or issues you've encountered related to communication session authenticity and how they were addressed.
- How do you validate the effectiveness of your mechanisms for ensuring communication authenticity?
- How do you stay informed about emerging threats or vulnerabilities related to communication session authenticity?

- Are there periodic security audits or assessments to validate the effectiveness of your communication authenticity mechanisms?
- How do you ensure that the approach to ensuring communication session authenticity aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L1-3.13.5

Derived

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

- How does your organization implement subnetworks for publicly accessible components?
- Describe the physical or logical separation mechanisms in place between these subnetworks and your internal networks.
- What tools or platforms do you use to manage and monitor these separated subnetworks?
- How do you ensure that traffic between the public subnetworks and internal networks is securely managed and monitored?
- Are there specific security controls or firewalls in place to prevent unauthorized access from the publicly accessible subnetworks to the internal networks?
- How frequently do you review and update the configuration and security measures of these subnetworks?
- Describe the process for granting and managing access between the subnetworks and the internal networks.
- How do you handle potential vulnerabilities or threats detected on the publicly accessible subnetworks?
- How do you ensure that third-party services or components on these subnetworks don't introduce vulnerabilities to the internal networks?
- Are there automated alerts or mechanisms in place to detect and respond to security incidents on the subnetworks?
- How do you manage data flow and storage between publicly accessible subnetworks and internal networks?
- Describe any challenges or issues you've faced related to managing these subnetworks and how they were addressed.
- How do you ensure that the security measures on the subnetworks do not inadvertently hamper legitimate access or functionality?
- How do you handle backup, recovery, and resilience for the publicly accessible subnetworks?

- Are there periodic security audits or assessments to validate the integrity and security of these subnetworks in relation to the internal networks?
- How do you train and educate relevant personnel about the importance and procedures related to managing the separated subnetworks?
- How do you stay updated on best practices and industry standards related to managing publicly accessible subnetworks?
- How do you ensure continuity of service and security during updates, migrations, or changes to the subnetworks?
- How do you handle feedback or concerns from stakeholders or users related to the accessibility or performance of the publicly accessible subnetworks?
- How do you ensure that the approach to managing and separating these subnetworks aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.4

Derived

Prevent unauthorized and unintended information transfer via shared system resources.

- How do you manage and monitor access to shared system resources?
- What controls are in place to prevent unauthorized information transfers through shared resources?
- Describe the mechanisms used to segregate data or processes within shared system resources.
- How do you ensure that users can only access and transfer data for which they have permissions in shared environments?
- What tools or platforms are employed to detect and alert on unauthorized information transfers?
- How do you handle shared resources in virtualized or cloud environments to prevent unauthorized data transfers?
- Are there any logging mechanisms specific to shared resource access and data transfers? If so, how frequently are these logs reviewed?
- How do you manage third-party access to shared resources to ensure they don't inadvertently transfer unauthorized information?
- What training or awareness programs are in place to educate users about the risks and protocols related to shared system resources?
- How do you ensure that shared resources, like printers or shared drives, are not misused for unauthorized data transfers?

- Describe any challenges or issues you've faced related to unauthorized transfers in shared resources and how they were addressed.
- How do you test or validate the effectiveness of controls placed on shared system resources?
- Are there specific protocols for highly sensitive data in the context of shared resources?
- How do you manage feedback or concerns from stakeholders related to shared resource access and data transfers?
- How do you handle data remnants or potential data leakage in shared resource environments?
- How do you integrate shared resource controls with other security systems, like Data Loss Prevention (DLP) tools or intrusion detection systems?
- How do you ensure that shared system resources are updated or patched without compromising their data segregation controls?
- Are there periodic security audits or assessments focused on shared resource controls and unauthorized data transfers?
- How do you handle incidents or breaches related to unauthorized data transfers in shared resources?
- How do you ensure that controls on shared system resources align with NIST guidelines and the broader cybersecurity objectives of the organization?

System and Communications Protection

SC.L2-3.13.3

Derived

Separate user functionality from system management functionality.

- How does your organization differentiate between user functionality and system management functionality in its systems and applications?
- What mechanisms are in place to ensure that regular users cannot access system management functions?
- Describe the tools or platforms used to enforce this separation of functionalities.
- How do you ensure that system administrators or those with management functionality cannot perform regular user functions under the same account or session?
- Are there distinct interfaces or portals for users and system administrators?
- How do you handle shared roles or accounts that might need both user and management functionalities?
- How do you audit or monitor access to system management functions to ensure only authorized individuals can use them?
- What training or awareness programs are in place to educate system administrators about the

importance of separating their roles from regular user roles?

- How do you manage third-party or external personnel who might need system management functionalities?
- Describe any challenges or issues you've faced in implementing this separation of functionalities and how they were addressed.
- Are there automated alerts or mechanisms to detect and respond to potential violations of this separation principle?
- How do you integrate the enforcement of this separation with other security measures, such as multi-factor authentication or logging?
- How frequently do you review and refine your approach to separating user and system management functionalities?
- How do you ensure that software updates, patches, or new system implementations adhere to this separation principle?
- Are there specific protocols or measures for critical or sensitive systems to further reinforce this separation?
- How do you handle exceptions or scenarios where temporary overlap of functionalities might be required?
- How do you test or validate the effectiveness of mechanisms enforcing the separation of user and management functionalities?
- How do you stay updated on industry best practices or recommendations related to this separation of functionalities?
- Are there periodic security audits or assessments to ensure consistent and effective separation of user and management functionalities?
- How do you ensure that the approach to separating functionalities aligns with NIST guidelines and the organization's broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.2

Basic

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

- How do your architectural designs incorporate information security principles?
- Describe the software development techniques you employ to ensure system security.
- What systems engineering principles do you utilize to enhance information security within your systems?

- How do you ensure that security is considered in the earliest stages of system design and development?
- Are there specific secure coding practices or guidelines that your development teams follow?
- How do you handle third-party components or software in terms of security design and validation?
- Describe any security frameworks or models that guide your architectural and design decisions.
- How do you ensure that security considerations are consistently applied across different systems or projects?
- What tools or platforms do you use to validate and verify security features during the development phase?
- How do you handle the trade-offs between functionality, performance, and security in system design?
- How do you ensure that security architecture and design considerations evolve with emerging threats and technologies?
- How do you integrate security considerations with other architectural concerns like scalability, availability, and usability?
- Describe any challenges or issues you've faced related to security in system design and how they were addressed.
- How do you collaborate with external entities, industry peers, or security experts on best practices in secure design and development?
- Are there periodic security assessments or reviews focused on architectural and design decisions?
- How do you educate and train your development and engineering teams on secure design principles?
- How do you ensure that legacy systems or existing solutions are aligned with current secure design and development principles?
- How do you manage feedback or concerns related to security implications of system design decisions?
- How do you measure the effectiveness of your security-focused architectural and design practices?
- How do you ensure that the approach to secure design and development aligns with NIST guidelines and the broader cybersecurity objectives of your organization?

System and Communications Protection

SC.L1-3.13.1

Basic

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.

- What mechanisms and tools do you use to monitor communications at the external boundaries of your systems?
- How do you identify and establish key internal boundaries within your organizational systems?
- Describe the controls in place to protect information transmitted across these boundaries.
- How do you ensure the integrity and confidentiality of information during transmission?
- What protocols and technologies are employed for encrypting data in transit?
- How do you detect and respond to unauthorized or suspicious communications at these boundaries?
- Are there specific firewalls, intrusion detection systems, or intrusion prevention systems deployed at these boundaries?
- How frequently are the configurations of these monitoring and control tools reviewed and updated?
- Describe any segmentation or isolation strategies employed to separate sensitive or critical system components.
- How do you manage and control communications involving third-party vendors or external partners?
- Are there automated alerts or mechanisms in place to detect potential breaches or exfiltration attempts?
- How do you ensure that remote access communications are also monitored and protected?
- Describe the process for updating or patching communication protection tools and ensuring they remain effective against evolving threats.
- How do you handle encrypted traffic inspection and management at these boundaries?
- What measures are in place to ensure the availability and resilience of communications, especially during high-traffic periods or potential denial-of-service attacks?
- How do you manage and control wireless communications within and across these boundaries?
- Are there periodic security audits, tests, or assessments to validate the effectiveness of communication protection mechanisms?
- How do you train and educate relevant personnel about the importance and best practices of communication protection?
- Describe any challenges or incidents related to communications protection you've encountered, and how they were addressed.
- How do you ensure that your approach to monitoring, controlling, and protecting communications aligns with NIST guidelines and broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.8

Derived

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

- What cryptographic mechanisms do you currently employ to protect CUI during transmission?
- How do you ensure that these cryptographic mechanisms meet or exceed NIST-approved standards?
- Are there any instances where CUI is transmitted without cryptographic protection? If so, what alternative physical safeguards are in place?
- How do you manage and protect cryptographic keys used for encrypting CUI during transmission?
- How do you ensure that third-party vendors or partners also employ adequate cryptographic protections when transmitting CUI?
- What protocols are in place to handle potential breaches or unauthorized disclosures of CUI during transmission?
- How often do you review and update your cryptographic mechanisms in light of evolving threats and best practices?
- How do you handle legacy systems or platforms that may not support the latest cryptographic standards?
- Describe the training or awareness programs in place to ensure personnel understand the importance of encrypting CUI during transmission.
- How do you validate the effectiveness and integrity of your cryptographic mechanisms?
- What methods are used to ensure secure key exchange or handshakes during encrypted transmissions of CUI?
- How do you handle situations where encrypted CUI transmissions need to be decrypted and inspected for security reasons?
- Are there automated alerts or mechanisms in place to detect potential unauthorized disclosures of CUI during transmission?
- How do you manage the lifecycle of cryptographic keys, including generation, storage, rotation, and disposal?
- Are there specific challenges or issues you've faced related to encrypting CUI during transmission, and how were they addressed?
- How do you stay updated on industry best practices and recommendations related to cryptographic protections for CUI transmission?

- In scenarios where encryption is not feasible, how do you ensure that alternative physical safeguards effectively protect CUI during transmission?
- How do you ensure compatibility and secure transmission of CUI when dealing with external entities or systems that might use different cryptographic standards or mechanisms?
- Are there periodic security audits or assessments to validate the consistent and effective encryption of CUI during transmission?
- How do you ensure that the approach to encrypting CUI during transmission aligns with NIST guidelines and the organization's broader cybersecurity objectives?

System and Communications Protection

SC.L2-3.13.16

Derived

Protect the confidentiality of CUI at rest.

- What encryption methods do you employ to protect CUI when it's stored or at rest?
- How do you determine where CUI is stored within your organization's systems and databases?
- How frequently do you audit and verify the encryption of CUI at rest?
- What measures are in place to detect and respond to unauthorized access attempts to stored CUI?
- How do you manage encryption keys, and what is their lifecycle?
- Are there specific standards or protocols that you adhere to for encrypting CUI at rest?
- How do you ensure that backups or replicas of CUI data are also encrypted and protected?
- What access controls are in place to restrict access to CUI storage locations?
- How do you handle decommissioning or disposal of storage devices containing CUI to ensure data confidentiality?
- Are there any exceptions or scenarios where CUI might be stored without encryption? If so, how are they justified and managed?
- How do you ensure third-party vendors or cloud service providers adhere to your standards for protecting CUI at rest?
- Describe any challenges or issues you've faced related to protecting CUI at rest and how they were addressed.
- How do you handle cases where encryption of CUI at rest might affect data accessibility or system performance?
- How do you stay updated on best practices and industry standards related to protecting CUI at rest?
- Are there periodic security audits or assessments to validate the protection of CUI at rest?

- How do you train and educate relevant personnel on the importance and methods of protecting CUI at rest?
- How do you ensure redundancy and availability of CUI data while maintaining its confidentiality at rest?
- How do you integrate protection measures for CUI at rest with other security tools or data management systems?
- How do you manage and monitor logs related to access and modifications of stored CUI?
- How do you ensure that your approach to protecting CUI at rest aligns with NIST guidelines and broader cybersecurity objectives?

WHY REDSPIN

- Over 100 security advisors and assessors, ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including multiple Joint Surveillance Voluntary Assessment Program (JSVAP) assessments
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com