3. Tailored Security Control Specifications

The total 60 security controls are either supplemented with additional guidance and/or augmented with discussions. In this section, these tailored security controls are categorized into 14 groups and presented in subsections for easier comparison.

3.1. Role-Based Access Control

AC-2, Account Management

Discussion for All Zones: An account's role should dictate its access to the HPC system and specific zones.

Supplemental Guidance for the Access Zone: This zone should be accessible to all authorized accounts, including users and system administrators.

Supplemental Guidance for the Management Zone: This zone is only accessible to system administrators.

Supplemental Guidance for the Computing Zone: This zone can be accessed by system administrators and user accounts that are authorized by the batch scheduler. Authorized users can only access high-performance computing nodes that have been assigned by the batch scheduler.

Supplemental Guidance for the Data Storage Zone: This zone is only accessible to system administrators.

Discussion for the Data Storage Zone: The data storage zone provides data service to the other zones. Users can access the data services via data service Application Programming Interfaces (APIs) but cannot log directly into the data storage servers/nodes. A good example of an API to the storage system is by using a mounted POSIX file system.

AC-3, Access Enforcement

Supplemental Guidance for All Zones: In HPC, the access privileges granted on one zone may not be automatically cascaded to another zone.

AC-6(5), Least Privilege | Privileged Accounts

Discussion for All Zones: In addition to the principle of least privilege, the privileges assigned to users and system administrators should be appropriate for their roles. The number of separate roles and accounts for system administrators should align with local policy. For instance, system administrators with root access should not — by policy — run user-type jobs in the computing zone. Rather, system administrators should have separate general user accounts for regular user tasks. System administrators may also schedule system maintenance jobs (e.g., performing rolling upgrades) with root privileges using a scheduler.

AC-17(4), Remote Access | Privileged Commands and Access

Supplemental Guidance for the Management Zone: There should be an organizationally defined and approved path to connect to the management zone, such as a gateway or bastion host.

Access to the Management Zone from other zones should be restricted, and these access paths should not overlap with user access paths. For instance, separate networks or VLANs should be used for login access and API access to the Management Zone.

3.2. HPC Logging

AC-6(9), Least Privilege | Log Use of Privileged Functions

Discussion for All Zones: Reducing the logging of privileged functions may pose a more significant risk than summarizing or discarding other logging events. Organizations should carefully consider this risk when evaluating the need to reduce logging. See AU-2 for further discussion.

AU-2, Event Logging

Supplemental Guidance for All Zones: Organizations should examine logging events to ensure that there is no duplicate logging. They may also consider reducing the logging event set with tolerable risks to ensure HPC system performance.

Discussion for All Zones: Parallelization in HPC environments may result in duplicated logging of the same event, and the large logging volume may negatively impact HPC system performance. For further guidance, see Office of Management and Budget (OMB) Memorandum M-21-31 [4] and the Cybersecurity and Infrastructure Security Agency (CISA) guide [5] for its implementation. Following the CISA guidance, there should be prioritized and detailed logging in the Management Zone over the Access Zone, and a lower priority should be given to the Data Storage Zone and the Computing Zone. Increase logging based on the priority list, and allocate resources (e.g., storage, performance) according to the risks that need to be managed through logging.

AU-3, Content of Audit Records

Discussion for All Zones: For further guidance, see OMB M-21-31 [4] and the CISA guide [5] for its implementation. Following the CISA guidance, the level of detail in logging in the Management Zone should be prioritized over the Access Zone, followed by the Data Storage Zone and the Computing Zone at the lowest priority. Increase logging based on the priority list, and allocate resources (e.g., storage, performance) according to the risks that need to be managed through logging.

AU-4, Audit Log Storage Capacity

Discussion for All Zones: The volume of logging in HPC systems can grow rapidly and unexpectedly. Organizations should customize their logging practices across different zones to effectively manage the volume of log data while also considering future logging requirements during procurements. Centralized logging is recommended for improved log retention and management.

AU-5, Response to Audit Logging Process Failures

Discussion for All Zones: The volume of logging in HPC systems can increase rapidly and unexpectedly. Organizations must be alerted early and respond promptly to prevent their logging systems from overflowing and causing potential cascading failures. A swift response to logging failures is particularly essential for HPC systems that include diskless nodes, as these nodes do not have local persistent storage to help them endure an outage of the centralized logging service.

AU-11, Audit Record Retention

Discussion for All Zones: Due to the system's size and complexity, the volume of HPC system log data can be enormous. Organizations are encouraged to consider different retention policies based on their log data's sensitivity and usefulness for audit purposes.

3.3. User Sessions

AC-2(5), Account Management | Inactivity Logout

Discussion for All Zones: While it is best practice to log out whenever possible, a logout may negatively impact ongoing work. In such scenarios, consider implementing compensatory measures to regulate access to the login session.

Supplemental Guidance for the Access Zone: The recommended logout time should align with the security policy for managing HPC user inactivity in the Access Zone. In HPC systems, it is crucial to distinguish a login session from the running processes that it controls. If it is feasible to log out of a session after inactivity without terminating the running process it controls, then the inactivity logout control can be implemented in HPC systems.

Discussion for the Access Zone: If the processes that run under the login session are separated from the remote login session, then the controlling remote session can be terminated without negatively affecting the running processes. Organizations can educate their users on utilizing tools such as GNU Screen [6] or *tmux* [7] to enable the separation.

Supplemental Guidance for the Computing Zone: The recommended logout time frame should conform to the security policy regarding user inactivity in the Computing Zone. Users who have active running jobs or processes should not be logged out. Access to compute nodes should only be terminated when the compute jobs are completed.

Discussion for the Computing Zone: User inactivity may occur while waiting for companion computing nodes to finish their tasks. Automatic user logout could lead to hanging jobs in the Computing Zone.

AC-10, Concurrent Session Control[3]

Supplemental Guidance for All Zones: The maximum number of allowed concurrent sessions in an HPC system may be set at a greater value at the organization's discretion. The maximum number of allowed concurrent sessions in different HPC zones may be set at different values.

Discussion for All Zones: Here, concurrent sessions refer to interactive concurrent sessions. Due to its scale and the number of interactive jobs that it supports, an HPC system generally requires more concurrent sessions than a typical enterprise system. Organizations are

[3] This control does not belong to the moderate security control baseline.

encouraged to conduct a proper risk assessment when choosing the maximum concurrent session threshold.

AC-12, Session Termination

Supplemental Guidance for the Access Zone: The selected session termination threshold should reflect the security policy for handling HPC user inactivity in the Access Zone. In general, the session termination threshold is set at a higher value than in typical enterprise systems.

Discussion for the Access Zone: Session termination terminates the user's interactive job and causes the user to lose their place in the scheduling queue. If the endpoints from which connections to the HPC system are made can be controlled, then a screen lock on the endpoint mitigates the risk of lengthening the termination threshold. Also, consider using tools that allow running processes to be disconnected from login sessions. In that case, the termination of the login session does not impact the running process.

Supplemental Guidance for the Computing Zone: The selected session termination threshold should reflect the security policy for handling HPC user inactivity in the Computing Zone. Sessions with current running jobs should not be terminated automatically in this zone.

Discussion for the Computing Zone: User inactivity may be caused by waiting for a companion compute node to finish processing the data. Terminating the session will lead to hanging jobs in the Computing Zone.

SC-10, Network Disconnect

Discussion for All Zones: Most HPC jobs can continue running even if the network connection is lost. This includes interactive debugging sessions, which may run for a long time. The debugging session should be managed using a tool that allows the running process to be temporarily disconnected from the login session. If the connection to that session is terminated, the user can still reconnect later.

3.4. HPC Backup

CP-1, Policy and Procedures

Discussion for All Zones: The contingency plan, policy, and procedures are heavily influenced by the mission of the HPC systems. For instance, research HPC systems may not be as critical as business support systems and may tolerate a longer outage period. Due to the cost of HPC systems, having a fully functional alternate site is often cost-prohibitive, and funds may be better spent making the primary site a more powerful system. Full data backup may also be prohibitive given the volume of the data and the fact that the intermediate results often change and have little innate value. Accordingly, HPC contingency plans may focus on reconstitution, reloading user input data from external authoritative sources, and ensuring that users are trained to promptly copy their output data (i.e., computational results) to external archives.

CP-6, Alternate Storage Site

Discussion for All Zones: It may not be feasible to back up all of the data in HPC systems. Configuration data and critical project information should be prioritized for backup at the alternate site to ensure that the HPC system can be restored to a functional state. The organization should identify critical data (e.g., user home directories, configuration management files) to be backed up at the alternate site. User training and contingency plans should clearly specify which data is backed up at the alternate site and which is not.

CP-7, Alternate Processing Site

Discussion for All Zones: Based on its needs and mission requirements, an organization may be unable to fund an alternate HPC system. Alternate processing sites may include processing sites at similar institutions via a Memorandum of Understanding (MOU) or utilizing the capabilities offered by cloud HPC service providers. An alternate processing site's architecture and capabilities may be different from the primary site as long as it satisfies the organization's mission requirements.

CP-9, System Backup

Discussion for All Zones: HPC systems typically have multiple data storage systems, some of which are designated as temporary or "scratch" and explicitly not backed up. Given the large volume of data in HPC systems, it may not be feasible to back up all data. Priority should be given to configuration data and critical project data to ensure that the HPC system can be restored to a functional state.

3.5. HPC Network Connections

AC-4, Information Flow Enforcement

Supplemental Guidance for All Zones: End-user access connections between external systems and the HPC system should be routed through the Access Zone. Such connections may need to support large data flows while following proper flow enforcement rules. The performance impact on the data flow due to security measures (e.g., firewall packet inspection, intrusion detection and prevention systems) may need to be accounted for and sometimes mitigated by doing the inspection on the replicated data flow while leaving the original flow unimpeded. The controlled interfaces within an HPC system should enforce the internal information flow rules.

CA-9, Internal System Connections

Discussion for All Zones: In this control, an HPC system with four zones is considered one unified system component. Communication connections between zones are outlined in SP 800-223 [3]. Within the Computing Zone, user jobs may set up connections between authorized processes that run on different nodes. These connections are confined to the Computing Zone and can be classified as authorized internal connections.

SC-8, Transmission Confidentiality and Integrity

Discussion for All Zones: An HPC system resides on an enterprise network. External connections include both the connections from the external internet to the HPC Access Zone and the connections from the enterprise network to the HPC Access Zone. Internal connections refer to connections inside the HPC boundary, as defined in SP 800-223 [3]. If this control cannot be effectively implemented in practice, compensating controls may serve as an alternative. For instance, encrypting traffic over internal connections may not be practical at this time. Compensating controls may use private, non-routable networks (e.g., for Message Passing Interface [4] jobs). Internal traffic encryption may become feasible in the future as hardware and software capabilities evolve.

SC-8(1), Transmission Confidentiality and Integrity | Cryptographic Protection

Supplemental Guidance for All Zones: No additional guidance is needed for transmissions over external connections. However, due to the nature of HPC, cryptographic protection may not be feasible for internal transmissions. See the discussions in SC-8 regarding alternative controls.

3.6. Identification and Authentication

IA-1, Policy and Procedures

Supplemental Guidance for All Zones: When developing policies and procedures, the unique requirements for accessing HPC systems should be properly considered and addressed.

Discussion for All Zones: HPC systems often have unique access requirements for the different zones. Organizations should consider accesses within the HPC system as single sign-on wherever appropriate.

IA-2(1), Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts

Supplemental Guidance for All Zones: Multi-factor authentication (MFA) should be required for access to the HPC system. However, once access is acquired, non-MFA connections among nodes within the HPC system may be permitted using the same identity. Changing identities within the system should also require MFA. Based on an organization’s policy, different zones may require MFA again.

IA-2(2), Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts

Supplemental Guidance for All Zones: MFA should be required for access to the HPC system. However, once access is acquired, non-MFA connections among nodes within the HPC system may be permitted using the same identity. Changing identities within the system should also require MFA. Based on an organization’s policy, different zones may require MFA again.

IA-2(12), Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Supplemental Guidance for All Zones: If Personal Identity Verification (PIV) is used to grant access to the HPC Access Zone, it should not be required again for internal access within the system. See IA-2(2).

Discussion for All Zones: Due to the large and diverse user base of HPC systems, organizations that require PIV as access identification (ID) may also consider accepting alternate forms of MFA for external users.

IA-11, Re-Authentication

Discussion for All Zones: Re-authentication could disrupt HPC user operations (e.g., interactive visualization, interactive debugging, multiple file downloading) and is often problematic due to the long-lived connections that exist in and between zones. This control is often tailored, and the time to re-authenticate is often set to infinity. Compensating controls (e.g., screen lock) can be introduced to mitigate the risks.

Supplemental Guidance for the Access Zone: This control should be carefully considered. See Sec. 3.3.

Discussion for the Access Zone: Login nodes often need to support long-lived sessions.

Discussion for the Management Zone: Management Zone access is typically limited to system administrators, and normal re-authentication should be enforced.

Supplemental Guidance for the Computing Zone: This control should be carefully considered. See Sec. 3.3.

Discussion for the Computing Zone: High-performance computing nodes need to support long-running jobs. Re-authentication will disrupt job execution.

Supplemental Guidance for the Data Storage Zone: This control must be enforced to ensure proper access for system administrators.

Discussion for the Data Storage Zone: HPC users access data, metadata, and file folders in the Data Storage Zone via file system clients, which make API calls to their corresponding file system servers for data retrieval. Users are not typically authorized to log into the Data Storage Zone directly and instead achieve access through service components. No additional authorization should be required once a user acquires initial access to the HPC system.

3.7. Emergency Handling

PE-11, Emergency Power

Supplemental Guidance for the Computing Zone: Depending on the HPC system's mission requirements, this control can either be enforced or tailored.

Discussion for the Computing Zone: The Computing Zone consumes a large volume of power. Hence, providing emergency power requires a significant investment. A job that is terminated due to a power interruption can restart, and the correctness of the job is not affected.

PE-15, Water Damage Protection

Discussion for All Zones: In addition to water being used in fire suppression systems, other cooling technologies may involve liquids that can damage equipment. The risks should be evaluated in the context of costs and potential damage, and a mitigation plan should be developed.

3.8. User-Developed Software

CM-7, Least Functionality

Discussion for All Zones: Many HPC systems support broad missions and often allow users to develop and run their own software. The least functionality can be difficult to achieve due to diverse user cases. User isolation technologies should be used to limit the effect of adverse software. This includes limiting user activities to and within the Access Zone and Computing Zone, thereby separating user activity from the more privileged and protected Data Storage Zone and Management Zone.

CM-7(1), Least Functionality | Periodic Review

Discussion for All Zones: Users should understand the different functionalities of each zone. The time period for conducting the least functionality control review should not exceed one year. Due to the sensitivity of and frequent changes in the Access Zone and Management Zone, a more frequent review (e.g., a quarterly review) should be considered.

CM-7(2), Least Functionality | Prevent Program Execution

Discussion for the Access Zone and Computing Zone: Many HPC systems cater to a variety of missions and often allow users to develop and run their own software. However, additional guidance and compensating controls may be necessary. For example, users should run their self-developed software in non-privileged mode, and it is important to consider implementing segregation among different programs and projects.

CM-7(5), Least Functionality | Authorized Software — Allow-by-Exception

Supplemental Guidance for the Access Zone and Computing Zones: Depending on the mission of an HPC system, a user’s self-developed software may be allowed to run. It may be impractical to maintain a list of explicitly allowed software when the mission of the HPC system allows users to bring in, develop, or compile software, as the list would need to be updated continuously to track user actions.

CM-11, User-Installed Software

Supplemental Guidance for the Access Zone and Computing Zones: User software is only accessible to individual users and their collaborators, while system-wide software can be used by all authorized users of a system. Additionally, software that requires special privileges to execute (e.g., software that needs access to privileged ports) is different from software that does not require any additional privileges. This control specifically pertains to non-privileged software that is used by a limited group of users. Users may be allowed to install and develop software that is necessary for their mission. They should create and manage this software in user space and regulate access for other users. Software that is installed system-wide is generally accessible to all users through a default path, while user-installed software is often accessed via specific paths. Users should not install software in the default path of any zone unless it complies with approved organizational policies.

Supplemental Guidance for the Management Zone and Storage Zone: Unprivileged user software should not be allowed in these zones.

SI-10, Information Input Validation

Discussion for All Zones: Users may be allowed to develop and run their own software on HPC systems that are designed to support a wide range of missions. For software created by users, it is crucial to follow safe and secure coding practices, adhere to acceptable use agreements, and implement security measures (e.g., input validation).

3.9. Impact on HPC Performance and Scalability

AC-8, System Use Notification

Supplemental Guidance for the Computing Zone, Management Zone, and Data Storage Zone: System use notifications (e.g., message of the day, legal banners) may be omitted at the organization's discretion to improve job output efficiency.

Discussion for the Computing Zone, Management Zone, and Data Storage Zone: Displaying system use notifications (e.g., message of the day, legal banners) adds an additional burden on users because they need to remove these messages from job output. In an HPC system, once users have accepted a system's use notification, further display in the other zones may be skipped at the organization's discretion.

SI-3, Malicious Code Protection

Supplemental Guidance for All Zones: This control may need to be tailored for different zones if it negatively impacts HPC performance or poses risks to the system's mission.

Discussion for All Zones: Real-time process scanning is the most effective approach for this control. Periodically scanning large file systems is often infeasible and negatively impacts storage system performance. Scanning shared resources from multiple compute nodes may also cause duplicate scans of the same data. The endpoints used by authorized users to access the HPC system are covered by organizational policies and are required to have malicious code protection installed to ensure that data is scanned prior to reaching the HPC system.

SI-4, System Monitoring

Discussion for All Zones: In HPC environments, there are often large, high-speed data flows to and from the Access Zone. These flows can overwhelm standard enterprise network monitoring tools. Internal networking may also require special consideration to collect the necessary information without negatively affecting the HPC system's performance or mission. See AU-2 for additional information.

SI-7, Software, Firmware, and Information Integrity

Supplemental Guidance for All Zones: This control is limited to system software, firmware, and information rather than user-installed software or user-managed information. System-wide installed software is accessible through the default path of all users, and software within specific domains is often accessed through specific paths. See CM-11.

Discussion for the Data Storage Zone: The parallel file systems in the Data Storage Zone often contain vast amounts of data and software, making it infeasible to conduct regular integrity checks on the entire file system.

CM-8(3), System Component Inventory | Automated Unauthorized Component Detection

Discussion for All Zones: Due to the size and complexity of HPC systems, automated inventory management scanning by enterprise tools from outside the HPC environment may lead to undesirable performance penalties and/or incorrect results. Out-of-band or idle-time assessment of the hardware components should be considered as alternatives.

CM-12(1), Information Location | Automated Tools to Support Information Location

Discussion for All Zones: While no additional guidance is needed, unintended impacts on the cost and performance of HPC systems should be considered during the control implementation.

RA-5, Vulnerability Monitoring and Scanning

Supplemental Guidance for All Zones: Due to the size and complexity of HPC systems, strategies should be developed to minimize the scanning overhead and possible scanning impacts on HPC processes and operations.

Discussion for All Zones: Scanning policies can be customized for different zones. Shared filesystems should avoid repeated scanning by multiple nodes. Given the filesystem size, data change rate, and/or scanning system load, scanning shared filesystems may not be feasible. HPC systems may also contain identical computing and data storage nodes. Scanning one node may be sufficient in this scenario. If a diskless system is employed, scanning one copy of the image is also sufficient.

3.10. Inapplicable to HPC

SC-15, Collaborative Computing Devices and Applications

Discussion for All Zones: This control is generally not applicable to HPC systems.

SC-18, Mobile Code

Discussion for All Zones: The use of mobile code is usually not found in HPC environments.

3.11. Shared GPUs and Accelerators

SC-4, Information in Shared System Resources

Supplemental Guidance for the Computing Zone: Computer systems that are equipped with accelerators (e.g., GPUs) should ensure that user data in the accelerator is cleared before being reassigned to the next user.

3.12. HPC-Specific Training and Security Overlay Tailoring

PL-11, Baseline Tailoring

Supplemental Guidance for All Zones: Using this overlay implies tailoring the selected baseline. Additional tailoring is possible as governed by organizational requirements.

AT-1, Policy and Procedures

Discussion for All Zones: Organizations are encouraged to develop HPC-specific documentation and training that captures their HPC system's unique characteristics.

AT-3, Role-Based Training

Supplemental Guidance for All Zones: HPC users and system administrators should receive HPC-specific training that is suitable for their roles.

Discussion for All Zones: The complexity and scale of HPC systems require skilled administrators and users. Users, administrators, and other organizational roles require additional training to facilitate communication between these specialized roles.

CA-2(1), Control Assessments | Independent Assessors

Discussion for All Zones: Due to the unique characteristics of HPC systems, assessors who are familiar with these systems will yield more effective assessment results.

3.13. HPC Management, Operation, and Maintenance

MA-6, Timely Maintenance

Discussion for All Zones: The time period threshold parameters defined by the organization may vary based on the criticality and impact of maintenance on the components in HPC systems, including software.

SI-2, Flaw Remediation

Discussion for All Zones: The organization-defined timing of fixing flaws may need special consideration for different HPC zones. For example, applying patches may be limited by vendor update schedules and the timing of integrating dependency patches from third-party sources. Additionally, both the Computing Zone and Data Storage Zone support long-running jobs that may exceed the organization-specified patch window, which requires special handling.

SI-5, Security Alerts, Advisories, and Directives

Discussion for All Zones: HPC-specific alerts may not be widely disseminated by default. HPC operators should subscribe to vendor-specific channels to receive relevant alerts about their systems.

CM-2(2), Baseline Configuration | Automation Support for Accuracy and Currency

Discussion for All Zones: Due to the complexity of HPC systems, baseline configuration automation support is important and may require professional resolution support.

CM-3(2), Configuration Change Control | Testing, Validation, and Documentation of Changes

Discussion for All Zones: Testing should be specific to the requirements of individual zones. For example, the Computing Zone should emphasize performance; the Access Zone should emphasize authentication and authorization; the Management Zone should emphasize a continuous monitoring capability; and the Data Storage Zone should emphasize data security and access performance. While a testing environment is important, it is often impractical to have a testing environment at the same scale as the production system or with the same specialized hardware components.

CM-9, Configuration Management Plan

Discussion for All Zones: The system configuration of a large-scale, complex HPC system is essential. A detailed system configuration plan is needed to describe the tight dependence among the zones and the components of the HPC system.

SC-5, Denial-of-Service Protection

Discussion for All Zones: Denial-of-service (DoS) detection methods for the nodes in the Access Zone are crucial. A denial of service can be caused by malicious attacks or a user erroneously using a system. Proper guidance and training should be provided to users to raise their awareness of the potential impacts of incorrect system usage. HPC system operators are encouraged to monitor the system and provide feedback to users.

SC-28, Protection of Information at Rest

Discussion for All Zones: For HPC systems, different protection approaches may be employed for various storage systems in different zones, accounting for performance impacts and security risks.

3.14. Access to HPC

AC-17(3), Remote Access | Managed Access Control Points

Discussion for All Zones: Due to their size and scale, HPC systems may quickly overwhelm the planned internet connection capacity. Organizations with Trusted Internet Connection (TIC) requirements should work closely with their TIC Access Provider (TICAP) to address the significant strains that HPC systems can place on organizational services.

AC-18, Wireless Access

Discussion for All Zones: Although users may wirelessly connect to the Access Zone, wireless access is not typically part of the HPC system.

AC-20, Use of External Systems

Discussion for All Zones: HPC systems typically have a far more permissive posture and descriptive process regarding the use of external systems than other systems in the organization. This control is often delegated to a team that is responsible for the organizational infrastructure and external connectivity. Organizations should prepare for detailed implementation of this control and corresponding enhancement controls to account for user trust, permissions, roles, and risks.

AC-20(2), Use of External Systems | Portable Storage Devices — Restricted Use

Discussion for All Zones: HPC systems typically have data transfer systems, which are preferred over portable storage devices. When required, connecting portable storage devices to HPC systems must follow organization-approved processes.

4. Summary

This HPC security overlay is based on the moderate security baseline in SP 800-53 with one additional control. The overlay has a total of 288 security controls, and 60 of them are tailored with supplemental guidance and/or discussion.

For many users, this overlay can serve as a starting point for securing their HPC systems. If necessary, users can further customize this security framework to meet their specific needs.