GRID DEPLOYMENT OFFICE

GRIP Training for Secured by Design Considerations

February 28, 2023

GRIP Training for Secured by Design Considerations

Colin Meehan

Project Manager, GRIP Program, Grid Deployment Office,
U.S. Department of Energy

GRID DEPLOYMENT OFFICE

GRIP Training for Secured by Design Considerations

David A. McKinnon

Senior Cyber Security Researcher,
Pacific Northwest National Laboratory

GDO
GRID DEPLOYMENT OFFICE

Pacific Northwest
NATIONAL LABORATORY

GRIP Training for Secured by Design Considerations

February 28, 2023

A David McKinnon, PhD, CISSP
Senior Cyber Security Researcher

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

GRIP Scope

- GRIP investments supports DOE, electric sector and all industry stakeholders' priorities that are focused on reliability, resiliency and security of the U.S. power grid.

- Security must be baked into the development process, not bolted on

- ***Security risk evaluation and mitigation measures should be an active component in a project (or product) lifecycle*** from early development stages to implementation

Security Assurance

- Physical security
  - Deter, detect, deny, delay, defend
- Cyber security
  - Integrity, availability, confidentiality
- Cyber-physical security
  - Defend against hybrid attacks
- Resilience
- Information assurance
- Supply chain risk management (hardware and software)

Source: pixabay.com

Perspective: What did the blind men see?

Lifecycle Support Considerations

- Cybersecurity risks and how they will be mitigated at each stage of the lifecycle
- Cyber security criteria utilized for vendor and device selection
- Relevant cyber security standards and/or best practices to be followed
- Plans for supporting emerging smart grid cybersecurity standard
- Ensuring confidentiality, integrity, availability
- Secure logging, monitoring, alarming, and notification
- Best practice to demonstrable evidence of the effectiveness of security controls

NIST Cybersecurity Framework

- Risk based, common approach
- Core Concepts
  - ***Identify*** – understand & manage cybersecurity risk to systems, people, assets, data, and capabilities
  - ***Protect*** – safeguards to ensure delivery of critical services
  - ***Detect*** – identify the occurrence of a cybersecurity event
  - ***Respond*** – act due to a detected cybersecurity incident
  - ***Recover*** – maintain resilience & restore any capabilities or services that were impaired due to a cybersecurity incident
- Implementation tiers
  - Partial
  - Risk-informed
  - Repeatable
  - Adaptive

https://www.nist.gov/cyberframework

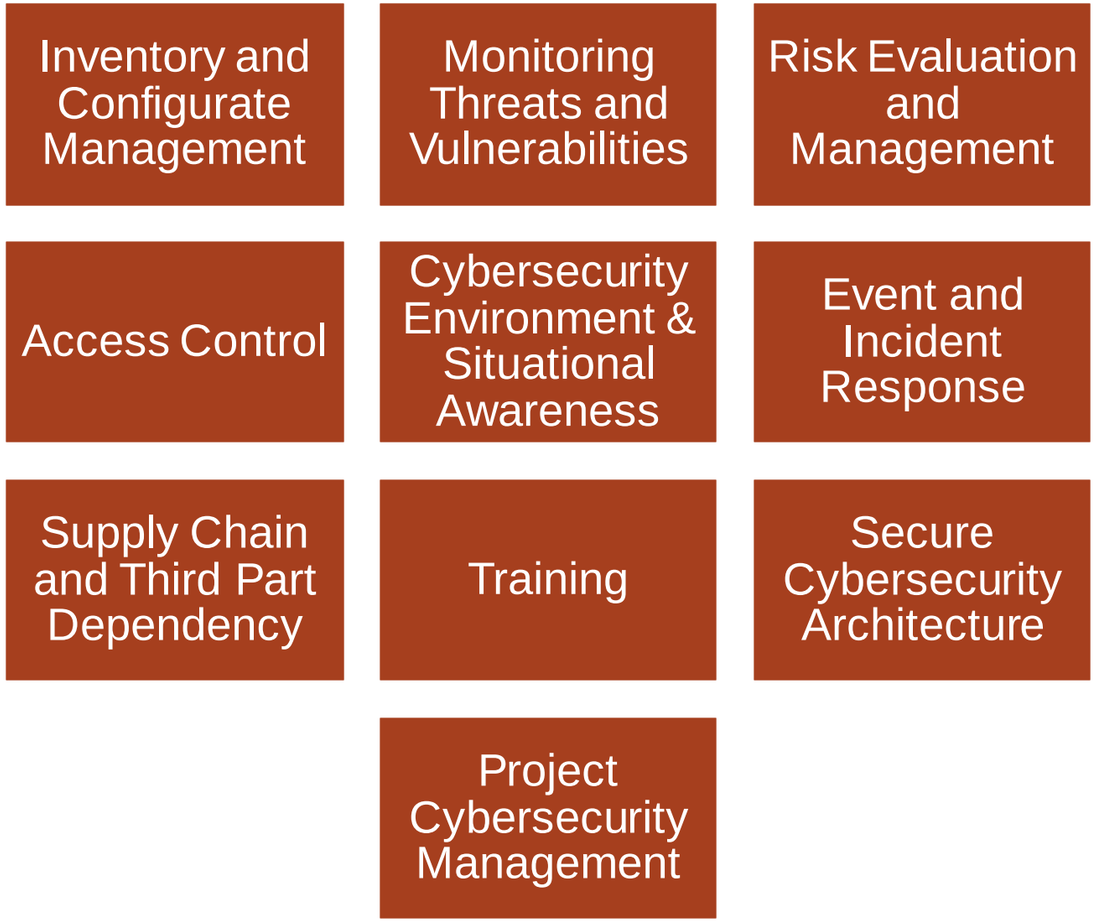
Cybersecurity Overview

- DOE may require any award or funding recipient to demonstrate the cybersecurity maturity of the project or solution and submit cybersecurity plan prior to issuance of funding
  - Specifies minimum contents of the Cybersecurity plan
  - Maximize use of open standards and guidance like C2M2
  - Document deviations or proprietary standards
  - DOE Program Office Coordination
    - ✓ DOE reviews plans to ensure integration with Department research, development, and demonstration programs

DOE will provide additional guidance on cybersecurity plans once the awards are selected. Recipients will be asked by the Sponsoring Program Office to complete their cybersecurity plan after they are selected for an award but before the funding is issued

Risk-Based Security Principles

- Apply defense in depth to address project risks
- Implement layered security mechanisms to increase the security of the systems as a whole
- Apply multiple security controls that can address the same concern from different security perspectives.



Cybersecurity Principles

- Project teams are encouraged to outline a plan of action for cybersecurity
  - Guide for project teams to follow when structuring a risk-appropriate plan
  - Create a comprehensive plan to protect their project's computer networks and systems
  - Ensures that the important elements are included
- Project teams should create a manageable plan
- Recipients are encouraged to leverage existing DOE tools and resources
- The Department recommends using open standards and guidance
  - For example, National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) and DOE's Cybersecurity Capability Maturity Model (C2M2 v2.1)
  - Justify and document the use of proprietary standards

Asset, Change, and Configuration Management

Maintain an inventory and configuration management of the digital assets and systems used in the project

i. What are the project's assets and critical assets?
    i. *Provide a high-level description of the types of assets that are part of the project.*

ii. What is the project team's plan to implement and maintain an asset inventory (including both IT and OT assets), provide configuration management, and govern the change control process?
    i. *Provide a high-level description of the plan and its commitment to develop and implement relevant policies and procedures.*

iii. Which security standards, guidelines, industry best practices, or guidance, etc. (if applicable) are the project team planning to use to support project team management of digital assets?

iv. Describe how the project team plans to assign proper resources (people, funding, and time), roles, and responsibilities for managing digital assets and systems?

Threat and Vulnerability Management

Outline a plan to monitor threats and cybersecurity vulnerabilities in project systems and assets

i. What is the project team's plan to identify and address project security vulnerabilities and security threats (threats)?
    i. *Provide a high-level description of the plan and the project team's commitment to identify and address vulnerabilities and threats.*

ii. Which standards, guidelines, industry best practices, or guidance, etc. (if applicable) is the project team planning to use to manage security threats and vulnerabilities?

iii. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing security vulnerability and security threats?
    i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Risk Management

Outline a plan to evaluate project security risks and make risk management decisions

i. What is the project team's plan to identify and address project cyber risks?
    i. *Provide a high-level description of the plan and its commitment to identify and address cyber risks.*

ii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will be used to support the project risk management program.

iii. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing security risks?
    i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Identity and Access Management

Outline a plan to limit access to systems and assets used in the project

i. What is the project team's plan to establish identities (for people and assets) and manage authentication?
    i. *Provide a high-level description of the plan to establish identities and manage authentication.*
ii. What is the project team's plan to control access (including logical/electronic and physical access) to the project's key systems and critical assets?
    i. *Provide a high-level description of the plan to control access.*
iii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will be used to support the project access management program?
iv. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing access to systems and assets?
    i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Situational Awareness

Outline a plan to monitor the security environment and maintain situational awareness.

i. What is the project team's plan to conduct monitoring (logging and analysis) activities to identify potentially malicious activity on its systems?
    i. *Provide a high-level description of the plan and its commitment to develop and implement relevant policies and procedures.*

ii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will be used to support the project's situational awareness program?

iii. What is the Project team's plan to assign proper resourcing, roles, and responsibilities for managing situational awareness activities?
    ii. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Event and Incident Response, Continuity of Operations

Outline a plan to respond to security events and incidents

i. What is the project team's plan to detect, characterize, and respond to security events?
ii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) is the project team planning to use to support its security event and security incident response program?
iii. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing the program's response to security events and incidents?

Supply Chain and Third-Party Risk Management

Outline a plan to address security supply chain issues and third-party dependencies

i. What is the project team's plan to identify and manage security risks associated with its supply chain and third parties (e.g., partners, contractors, or service providers who have access to internal company or customer data, systems, processes, or other privileged information)?
    i. *Provide a high-level description of the plan and its commitment to manage the security risks associated with the supply chain and third parties.*

ii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will be used to support the project's management of supply chain and third-party risk management program?

iii. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing the security risks associated with its program's supply chain and risk involving third parties?
    i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Training

Outline a plan to prepare the project team to recognize and address security issues

i. What is the project team's plan to provide security training and awareness activities for its workforce?
   i. *Provide a high-level description of the plan and its commitment to provide security and awareness activity for the project workforce.*

ii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will the project team use to support the project workforce training and awareness program?

iii. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing the security risks associated with its project's workforce?
   i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Cybersecurity Architecture

Outline a plan to implement and maintain a secure project cybersecurity architecture

i. What is the project team's plan to implement proper network protections as an element of the project's cybersecurity architecture?
    i. *Provide a high-level description of the plan and its commitment to implement appropriate network protections.*

ii. What is the project team's plan to implement software and data security as an element of the cybersecurity architecture?
    i. *Provide a high-level description of the plan and its commitment to develop and implement software and data security.*

iii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will the project team use to support the project's cybersecurity architecture program?

iv. What is the project team's plan to assign proper resourcing, roles, and responsibilities for managing activities related to maintaining a secure cybersecurity architecture?
    i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Security Program Management

Outline a plan to allocate resources and assign roles and responsibilities for project management

i. What is the project team's plan to manage the project's security program?
   i. *Provide a high-level description of the plan for the overall management of the project's cybersecurity program.*

ii. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will the project team use to support you're the project's cybersecurity management program?

iii. What is the project team's plan to assign proper resourcing, roles, and responsibilities for the management of security?
   i. *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

Secure Design Principles to Adopt

Several well-known secure design principles could be applied to modernized power systems and distributed energy resources (DER) environments

Eight of these secure design principles are:

Defense in Depth

Implement layered security mechanisms to increase the security of the systems as a whole

Apply multiple security controls that can address the same concern from different security perspectives

Secure Design Principles to Adopt, continued

Principle of Least Privilege

Provides users, programs, and processes only with necessary privileges to complete their tasks

- Only offer the minimum required access for each authorized user to resources they absolutely need
- Access should be granted only for as long as necessary to complete that work.

When properly implemented, least privilege will substantially reduce the risk of cascading failure of utility operations caused by multiple devices being compromised through a single device compromise. Such cascading failures scenarios are well known and well described elsewhere

Principle of Least Functionality

Restrict the functions that users and devices are allowed to access to only those required to perform a task or function

- Reduces potential vulnerabilities and remove potential points of attack.
- Applies to both access to the device itself and to the functions running on the device

Examples include

- Enforcing use of specific protocols
- Removal of default settings
- Disabling services and functionalities that are not required

When properly implement, least functionality will reduce a system's attack surface

Secure Design Principles to Adopt, continued

Zero Trust

Assume that there is no implicit trust granted to devices or user accounts based solely on their physical or network location or ownership

The overall system needs to be designed to trust devices only by continuously authenticating their identity and confirming the functions they are authorized to perform

Continuity of Operations

Operate under the assumption that a breach is inevitable

- Anticipate and plan for breaches
- Prepare to withstand and recover from a breach

If a breach occurs, operations should continue–even if at a diminished capacity–until the breach is resolved

Secure Design Principles to Adopt, continued

Data minimization

Limit the collection and processing of data to only what is required to fulfill a specific purpose

Implement appropriate technical and organizational protection measures to limit data collection

Configuration Management

Verify all system security settings

- Do not rely on default security settings
- Change settings based on what is required for utility operations

Backup system configurations as part of a holistic disaster recovery plan

Fail Secure

When a failure occurs, the system should not fail into a compromised or vulnerable state

Resources

- Outline the plan to maintain an inventory and configuration management of the digital assets and systems used in the project
  - NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
  - https://csrc.nist.gov/publications/detail/sp/800-128/final
- Outline the plan to monitor Cybersecurity Threats and Cybersecurity Vulnerabilities in Project team digital systems and assets.
  - NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
  - https://csrc.nist.gov/publications/detail/sp/800-137/final
- Outline the plan to evaluate project Cybersecurity Risks and make Risk Management decisions
  - NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
  - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- Outline the plan to limit access to systems and assets used in the project
  - NIST IR 7316, Assessment of Access Control Systems
  - https://csrc.nist.gov/publications/detail/nistir/7316/final

Resources, continued

- Outline the plan to monitor the Cybersecurity Environment and maintain situational awareness.
  - NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems & Org.
  - https://csrc.nist.gov/publications/detail/sp/800-137/final
  - NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
  - https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- Outline the plan to respond to Cybersecurity Events and Cybersecurity incidents.
  - NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
  - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Outline the plan to address Cybersecurity Supply Chain issues and Third-Party dependencies.
  - NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Orgs.
  - https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
  - NIST SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning: Preventive Maint. for Technology
  - https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final
  - Cybersecurity Supply Chain Risk Management
  - https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications
  - Cybersecurity Procurement Language for Energy Delivery (April 2014)
  - https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014

Resources, continued

- Outline the plan to prepare project team to recognize and address cybersecurity issues.
  - NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
  - https://csrc.nist.gov/publications/detail/sp/800-50/final
- Outline the plan to implement and maintain a secure project cybersecurity architecture.
  - NIST SP 800-37 r2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
  - https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
  - NIST SP 800-18 Rev. 1. Guide for Developing Security Plans for Federal Information Systems
  - https://doi.org/10.6028/NIST.SP.800-18r1
  - Energy Sector Cybersecurity Framework Implementation Guide
  - https://www.energy.gov/ceser/downloads/energy-sector-cybersecurity-framework-implementation-guidance
- Outline the plan to allocate resources and assign roles and responsibility for Project cybersecurity management.
  - NIST SP 800-37 r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
  - https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
  - NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Informat. System View
  - https://csrc.nist.gov/publications/detail/sp/800-39/final

Conclusion

- Security must be baked into the development process, not bolted on
  - Use a holistic, security assurance approach

- Security risk evaluation and mitigation measures should be an active component throughout a project's (or product's) lifecycle
  - Development
  - Implementation
  - Operation
  - Decommissioning

Thank You!