Cyber Security Strategy and Roadmap Template

Annabelle Lee

Chief Cyber Security Specialist

Nevermore Security

December 2019

TABLE OF CONTENTS

LIST OF FIGURES

1 CYBER SECURITY STRATEGY OVERVIEW

The current power grid consists of both legacy and next generation technologies. These new components operate in conjunction with legacy equipment that may be several decades old and provide no cyber security controls. In addition, industrial control systems/supervisory control and data acquisition (ICS/SCADA) systems were originally isolated from the outside world. Sensors would monitor equipment and provide that information to a control room center. As networking technology has advanced and become more accessible, utilities have made decisions to integrate systems. This integration is necessary to take advantage of the new technology that is being deployed.

To adequately address potential threats and vulnerabilities, and develop an effective cyber security strategy, the utility needs to have a current architecture that includes the system assets, communication links, and connections to external systems. Knowing the system boundaries and the assets that are within the boundary may be used to determine what needs to be protected. Currently, with the increase in wireless communications and the connection of Industrial Internet of Things (IIoT) devices, the overall attack surface has increased.

A cyber security strategy includes an integrated strategy to reduce cyber risks by addressing high-priority objectives and activities that will be pursued over the next few years to reduce the risk of energy disruptions due to cyber incidents. Because of the constantly changing threat and technology environments related to the digital infrastructure, the typical time frame for the activities in the strategy is one to three or five years.

In addressing cyber security, achieving 100% security of all systems against all threats is not possible. The number of resources (including funds, staff, and technology) are limited and all systems cannot and should not be protected in the same manner. Risk-based methods should be used to make decisions and prioritize activities. Because threats will not diminish, energy delivery systems must be designed and operated so they can continue to perform critical functions during and after an attack. Finally, cyber security features should not interfere with the energy delivery functions of the devices and components they are meant to protect.

The purpose of this document is to specify a cybersecurity strategy and roadmap template that may be used by utilities. This document is NOT an attempt to develop new guidance but rather document the diverse existing guidance that is available to the electric sector.

1.1 Utility Cyber Security Program

The following figure includes the cyber security program components, including the cyber security strategy. As illustrated, the enterprise elements (vision, mission, and strategy; policies and regulations) should be developed first and then used as input to the development of the cyber security strategy elements that are further described in this document. (Note: the cyber security risk management framework and risk assessment are described in a companion document.)

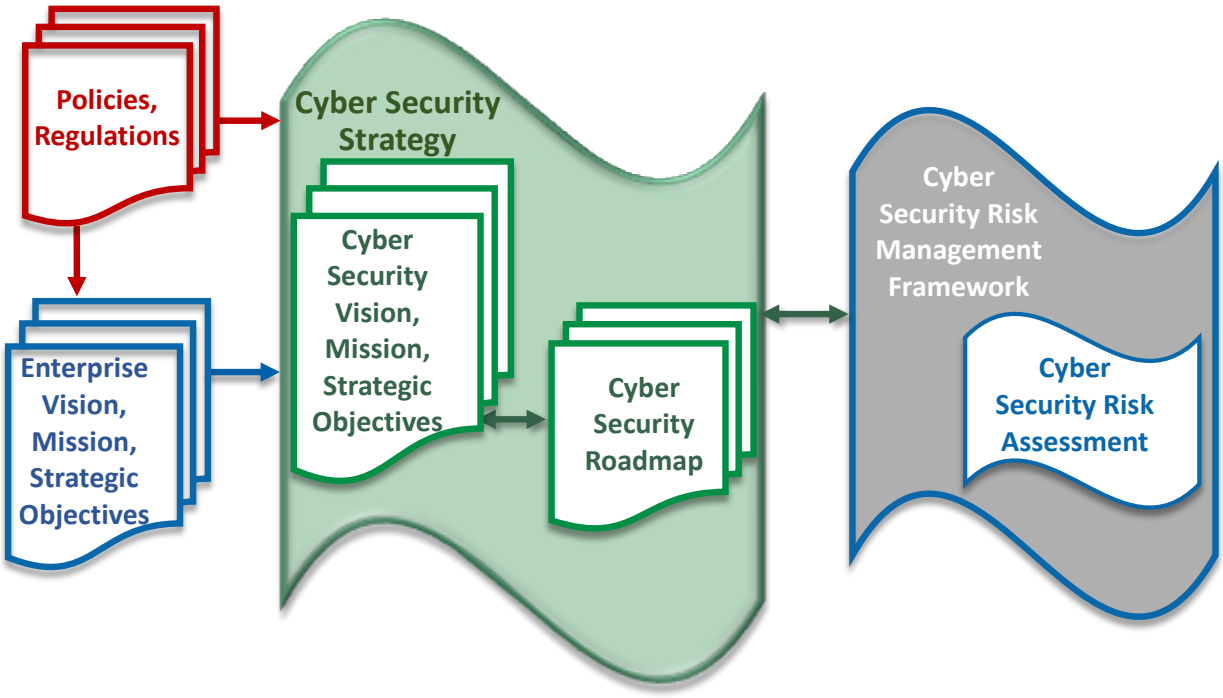


Figure 1: Cyber Security Program Components

The purpose of a cyber security strategy is to define the goals and objectives of the cyber security program to assure the confidentiality, integrity, and availability of the information vital to achieving the utility's mission. A cyber security strategy is a plan of action designed to achieve a long-term or overall aim of increasing the resilience, reliability, and security of the utility's IT and operational technology (OT) assets. The strategy should define the current status and the target goal and address the hardware, software, people and processes of the utility. A well-developed cyber security strategy may be used by a utility in making investment decisions and addressing risks to the various systems.

1.1.1 Policies and Regulations

Every organization must meet various regulations, and this includes all utilities. For the energy sector, regulations address, for example, energy security and privacy. *Policies* are the rules that the staff and other stakeholders follow as they perform their duties and some policies are based on regulations.

1.1.2 Enterprise Vision, Mission, and Strategic Objectives

Each utility should initially define the mission, vision, strategic objectives, and projects/activities to meet the strategic objectives. The following figure illustrates the hierarchy:

Figure 2: Organization Strategy Hierarchy

The vision and mission are at a high level, are based on the business functions of the utility, and generally don't change over time. They set the high level objectives that are to be accomplished. The strategic objectives should only be updated if there are significant changes in the threat and/or technology environments. Projects and activities are specific and should be defined and reviewed annually.

The *vision* is an aspirational description of what an organization would like to achieve in the future. Some examples are:

- Powering a new and brighter future for our customers and communities
- The utility will be recognized for excellence in the products and services provided to our customers and community

The *mission* is a statement of the organization's core purpose. Some examples are:

- The utility is a source of essential services which meet and exceed customer expectations through reliability, stewardship and technological advancement.
- Our mission to provide clean, safe, reliable and affordable energy

Strategic objectives convert the mission statement from a broad vision into more specific plans and defines the scope for the next few years.

1.1.3 Cyber Security Vision, Mission, and Strategic Objectives

The cyber security vision, mission, and strategic objectives should support the enterprise vision, mission, and strategic objectives of the utility, including reliability and resiliency.

Cyber security vision examples include:

- An agile, effective, and cost-efficient approach to cyber security aligned with current threats and adaptable to the organization's missions.

- Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Cyber security mission examples include:

- Enable improved mission accomplishment while strengthening the protection of systems and data
- To assure our mission when considering cybersecurity, the objectives of this strategy are to facilitate risk based decision-making that weighs trade-offs and supports action that:
    - Prevents cyber-attacks against critical infrastructures;
    - Reduces vulnerability to cyber attacks; and
- Minimizes damage and recovery time from cyber-attacks that do occur.

Cyber security strategic objectives should be continuously updated as projects are completed, and the organization is reassessing to establish new risk baselines. Listed below are example cyber security strategic objectives:

- Strengthen Energy Sector Cybersecurity Preparedness
    - Enhance information sharing and situational awareness capabilities
    - Strengthen risk management capabilities
    - Reduce critical cybersecurity supply chain vulnerabilities and risks

- Coordinate Cyber Incident Response and Recovery
    - Establish a coordinated national cyber incident response capability for the energy sector
    - Conduct cyber incident response training and improve incident reporting
    - Exercise cybersecurity incident response processes and protocols

1.1.4 Cyber Security Roadmap

At the lowest level, are the cyber security activities associated with each cyber security strategic objective. These activities should be documented in a roadmap. Included in the figure below is a roadmap template.

2019	2020	2021	2022	2023
• Activity 1 • Activity 2	• Activity 1 • Activity 2	• Activity 1 • Activity 2	• Activity 1 • Activity 2	• Activity 1 • Activity 2

Figure 3: Roadmap Template

The intent of a roadmap is to document the activities/projects by calendar year, typically three to five years. The focus of the activities is to meet the strategic objectives. The activities should include technology, processes, and/or procedures and measures of success.

1.1.5 Cyber Security Strategy Maintenance

A cyber security strategy should be owned/approved by a senior-level individual within the utility. The cyber security strategy is not a static document and should be updated at regular intervals to ensure that the content is current and that the mitigation strategies continue to be

effective. The figure below illustrates the process for developing and maintaining a cyber security strategy.

Figure 4: Cyber Security Strategy Development and Update[1]

1.2 Cyber Security Strategy Phases

1.2.1 Phase 1: Develop the Strategy

In Phase 1, the cyber security strategy is developed based on the enterprise cyber security strategy and policies, regulations, and standards. This includes developing the cyber security mission and vision. Because the cyber security strategic objectives are at a more detailed level than the mission and vision, it is important to determine the current cyber security status of the utility, as specified in the following steps.

1.2.1.1 Governance Framework

A governance framework includes the steps for the implementation, evaluation, and maintenance of the cyber security strategy.

1. The first step in the *governance framework* is to identify the individuals, roles, and organizations that are responsible for the tasks and the individual who is ultimately responsible for signing-off on the framework, typically a C-level executive. Relevant stakeholders include, for example, users, external vendors, contractors, third-parties, technical staff, and senior management. Management needs to understand that cyber security is an organization-wide issue, not just an IT (or OT) issue.

   Accountability is critical. The stakeholders identified above should be involved from a strategic perspective to gain commitment when the cyber security strategy is executed. Some of the roles are:

[1] This diagram is based on a diagram developed by ENISA in 2012.

1. *Chief Information Security Officer/Chief Security Officer*: C-level executive accountable for the security of the organization's systems to ensure that the business functions are protected.
2. *Security Analysts*: assess, plan, and implement security controls in the various systems and networks.
3. *Security Architects*: document and maintain the computer and network security infrastructures.
4. *Threat Analysts*: collect and analyze threat and vulnerability data.

2. The second step is to identify the current cyber security state of the utility, specifically the cyber security maturity using the Cybersecurity Capability Maturity Model (C2M2) developed by the United States Department of Energy (US DOE).
3. The third step is to develop a security architecture using any previously completed enterprise architecture that includes the hardware, software, network configurations, and external connections. The security architecture should include both the physical and logical connections. An enterprise architecture typically does not focus on cyber security. The security architecture should include all IT and OT systems in the utility.
    a. At a minimum, two security architectures should be developed – one documenting the current state and a second one documenting the target architecture. As required, additional architectures may be developed that document the transition phases between the current and target architectures.
4. The fourth step is to perform a threat assessment to identify threat agents, attack vectors, and potential vulnerabilities, using the architecture diagrams.
5. The fifth step is to review the security architecture and the threat assessment with all stakeholders for accuracy and revise, as required.
6. The sixth step is to identify the critical IT and OT systems. This step should be performed in collaboration with the various business function owners, for example, human resources, finance, transmission/distribution substation operators, and physical security.
7. The seventh step is to conduct a high level cyber security risk assessment. This assessment should be performed on the high priority/critical systems identified in step 6. The objective is to identify the cyber security gaps. The gaps should then be prioritized and used as input to the development of the cyber security strategy and the roadmap.
8. The eighth step is to define mitigation strategies.

1.2.2 Phase 2: Execute the Strategy

In Phase 2, the cyber security strategy is executed. As documented above, the roadmaps are developed in Phase 2 and define the specific activities that are intended to meet the strategic objectives and address cyber security gaps. This includes executing the various mitigation strategies, identifying the specific activities, developing timelines, and allocating the required resources. There may be several activities listed under each strategic objective. The activities include technologies, policies, and procedures. Finally, metrics/key performance indicators (KPIs) to measure progress should be developed.

1.2.3 Phase 3: Evaluate the Strategy

In Phase 3, the cyber security strategy is evaluated. The cyber security strategy should be evaluated at regular intervals, or when there is a significant change in technology or the threat environment. The objective is to determine the status of the strategy and identify modifications that need to be made to the mission, vision, strategic objectives, and activities. At the completion of an evaluation, a report should be developed and presented to senior management. Following is guidance in developing an evaluation strategy:

- Define the scope of the evaluation, the key objectives, and the frequency for performing the evaluation.
- Identify the position/roles and responsibilities of those who will perform the evaluation. This may be an individual (or individuals) or trusted third party that did not write the strategy. The assessment of activities may require individuals who are knowledgeable about the system and the security controls.
- Train the individuals to ensure that results are comparable across the evaluation teams.
- Benchmarking results should be developed to compare versions of the cyber security strategy. The goal is to document progress and identify new threats and cyber security risks.

At the completion of the evaluation, lessons learned, effective and ineffective practices, and gaps should be developed and used to update the strategy.

1.2.4 Phase 4: Monitor the Strategy

In Phase 4, the cyber security strategy is assessed based on audits and/or cyber security exercises. The goal of this phase is to ensure that the mitigation strategies continue to be effective. This is done by evaluating each activity against the KPIs and identifying gaps. Because utilities do not have unlimited resources, e.g., staff and funding, addressing gaps may include accepting or transferring the associated risk. Typically, audits are performed by individuals who did not author the cyber security strategy to ensure independence of the content. Results of the monitoring phase may require updates to the cyber security strategy.

1.3 Factors that Impact the Strategy

In addition to a changing threat and technology environment, there are other external and internal factors that may impact the cyber security strategy. The external factors are new threats and new and revised regulations and policies.

With grid modernization, utilities are revising their architectures to incorporate renewable resources and newer digital technologies at substations. These architecture changes will require changes to the various business functions. The architecture and business functions are internal factors.

As stated above, cyber security must be regularly assessed because of the constantly changing technology and threat environments. This includes assessment factors such as continuous monitoring to identify gaps in technology, processes, and procedures and ensuring that the mitigation strategies continue to be effective.

All these factors may require a revision to the cyber security strategy and are illustrated in the figure below.

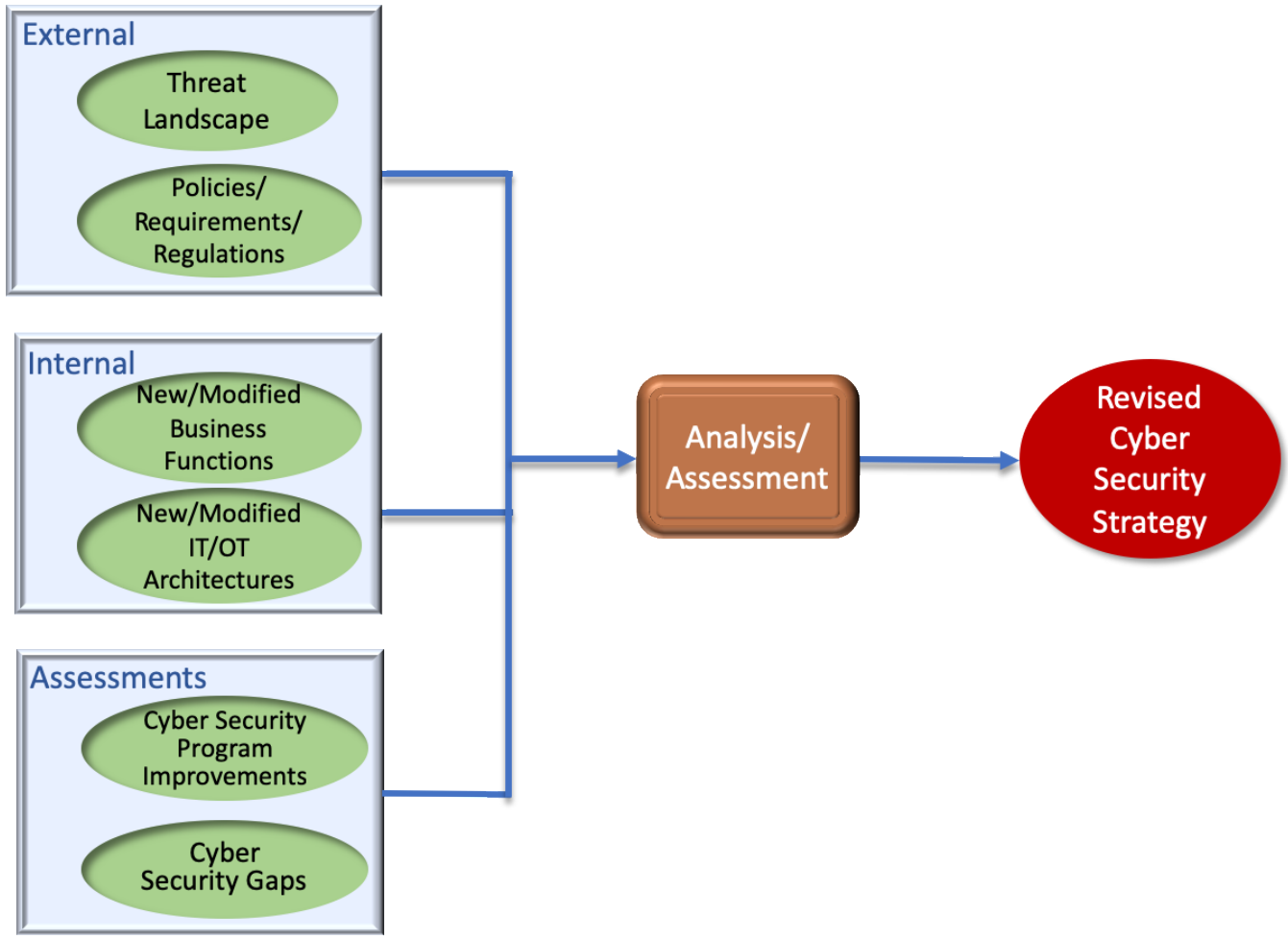


Figure 5: Updating the Cyber Security Strategy

2 SAMPLE CYBER SECURITY STRATEGY

Following is a completed cyber security strategy that may be used as a model.

Cyber Security Vision

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

Cyber Security Mission

Advance the utility's mission through:

- The development and adoption of cyber security policies
- Implementation of prioritized risk management-based cyber security mitigations
- Implementation of risk based decision-making that weighs trade-offs and supports actions that:
  - Reduce vulnerabilities to cyber attacks and
  - Minimize damage and recovery time from cyber-attacks that do occur

Cyber Security Strategic Objectives, Roadmap Activities, and KPIs

1. Strengthen utility cyber security preparedness:

    a. Increase cyber security through improved governance, policies, and oversight

Roadmap Activities

2020	2021	2022	2023	2024
Identify critical IT and OT systems	Develop target profiles using C2M2 assessment	Update interim profiles	Identify mitigation strategies for high impact vulnerabilities and attack vectors	Update C2M2 assessments
Conduct C2M2 assessments on critical IT and OT systems	Develop interim profiles using C2M2 assessments	Develop security architecture using enterprise architecture, including substation zoning		Revise target profiles
Develop 5-year roadmap, to address gaps	Develop/update enterprise architecture	Identify attack vectors and vulnerabilities of critical IT and OT systems		
		Perform audits of cyber security procedures and		

2020	2021	2022	2023	2024
		technical controls		

KPI/Metrics:

- Reports from the C2M2 assessments and the associated interim and target profiles.
- Criteria for identifying cyber security gaps
- Criteria for prioritizing IT and OT systems
- Five-year roadmap

b. Enhance information sharing and situational awareness capabilities

Roadmap Activities

2020	2021	2022	2023	2024
Establish information sharing platform	Whitelisting pilot for substations	Machine learning pilot for substations		Machine learning deployment at substations
Participate in public/private partnerships for information sharing		Whitelisting deployment		

KPI/Metrics:

- Criteria for identifying whitelisting applications
- Developed machine learning algorithms

2. Maintain an adequate level of cyber security commensurate with risk

Roadmap Activities

2020	2021	2022	2023	2024
Identify high priority risks based on C2M2 assessments	Develop threat profiles for OT systems	Deploy cyber security technical controls in critical IT and OT systems	Deploy cyber security technical controls in critical IT and OT systems	Deploy cyber security technical controls in critical IT and OT systems
Develop risk profiles for IT and OT systems	Identify and assess high priority technical controls for IT and OT systems, including cost and	Update threat and risk profiles for IT and OT systems		Update threat and risk profiles for IT and OT systems

2020	2021	2022	2023	2024
	performance impact			

KPI/Metrics:

- Criteria for identifying risks and threats
- Tests for assessing technical controls

3. Reduce critical cybersecurity supply chain vulnerabilities and risks

Roadmap Activities

2020	2021	2022	2023	2024
Identify critical vendors and suppliers	Update list of critical vendors and suppliers	Update list of critical vendors and suppliers	Update list of critical vendors and suppliers	Update list of critical vendors and suppliers
Review and revise procurement requirements and procedures to address supply chain risks		Review and revise procurement requirements to address supply chain risks		Review and revise procurement requirements to address supply chain risks
Identify supply chain technical controls, for example, integrity controls	Assess supply chain technical controls	Deploy supply chain technical controls		

KPI/Metrics:

- Procurement language that addresses supply chain risk
- Criteria for identifying critical vendors and suppliers

4. Conduct cyber incident response training and improve incident reporting

Roadmap Activities

2020	2021	2022	2023	2024
Develop tabletop exercise procedures and use cases	Conduct tabletop exercise	Conduct tabletop exercise	Conduct tabletop exercise	Conduct tabletop exercise
	Update tabletop exercise documentation based on lessons learned	Update tabletop exercise documentation based on lessons learned	Update tabletop exercise documentation based on lessons learned	Update tabletop exercise documentation based on lessons learned

KPI/Metrics:

- Tabletop exercises procedures and use cases
- Results and lessons learned from tabletop exercises

3 CYBER SECURITY STRATEGY TEMPLATES

Included below are several cyber security strategy templates. The content is the same across the templates, but the headings are different.

3.1 United States (US) Transportation Security Administration (TSA)

The TSA cyber security roadmap template includes the following:

- Mission
- Vision
- Priority 1
  - Goal 1.1
    - Objective 1.1.1
    - Outcome
- Priority 2
  - Goal 2.1
    - Objective 2.1.1
    - Outcome

Included below is sample content:

- *Mission:* Protecting the nation's transportation systems to ensure freedom of movement for people and commerce is the Transportation Security Administration (TSA)
- *Vision*: be an agile security agency, embodied by a professional workforce, that engages with its partners and the American public to outmatch a dynamic terrorist threat.
  - *Priority 2* – Vulnerability Reduction
    - *Goal 2.1*: Protect TSA Information Systems
      TSA will reduce vulnerabilities to ensure TSA's network, systems, and data are secure.
      - *Objective 2.1.1*: Increase cybersecurity of the TSA enterprise through improved governance, information security policies, and oversight.
      - *Outcome*: TSA maintains an adequate level of cybersecurity commensurate with our risk within the federal enterprise.
      - *Objective 2.1.2*: Provide protective capabilities, tools, and services across the TSA enterprise.

3.2 US Department of Homeland Security (DHS)

The US DHS cyber security strategy template includes the following:

- Pillar I
  - Goal 1
- Pillar II
  - Goal 2
  - Goal 3
- Guiding Principles
- Objective 1.1
  - Subobjectives
    a.
    b.
    c.
  - Outcomes

Included below is sample content:

- *Pillar 1* – Risk Identification
  - *Goal 1*: Assess Evolving Cybersecurity Risks
    We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.
    - *Objective 1.1*: Maintain strategic awareness of trends in national and systemic cybersecurity risks.
      - *Sub-Objectives:*
        - a. Identify evolving cybersecurity risks that affect national security, public health and safety, and economic security
        - b. Identify and develop plans to address gaps in analytic capabilities and risk management efforts across DHS and national cybersecurity stakeholders.
        - c. Develop scenarios and plans for future technology developments and potentially disruptive innovations and adjust DHS efforts accordingly.
  - *Outcomes:* DHS understands national and systemic cybersecurity risks and regularly adjusts our program and policy efforts to account for evolving technologies and operational priorities.
- *Guiding Principles*: DHS advances our mission and will accomplish our cybersecurity goals by aligning departmental activities according to the following guiding principles:

1. *Risk prioritization*
2. *Cost-effectiveness*
3. *Innovation and agility*
4. *Collaboration*
5. *Global approach*
6. *Balanced equities*
7. *National values*

3.3 US Department of Energy (DOE)

The US DOE cyber security strategy template includes the following:

- Cybersecurity Vision
- Cybersecurity Mission
- Crosscutting Principles
- IT Goal 1
    - Objective 1.1
        - Major Tasks
        a.
            1)
            2)
- 2018 Performance Plan
    - Objective
    - Performance Goal (Measure)
    - Endpoint Target
    - 2019 Target
    - 2020 Target
- Key Challenges

Included below is sample content:

- *Cybersecurity Vision*: Many missions working together as one efficient and effective enterprise to provide best-in-class security across the Department of Energy.
- *Cybersecurity Mission*: Advance the Department's mission through the collaborative development and adoption of enterprise-wide cybersecurity policies matched by prioritized risk management-based implementation of cybersecurity defenses that enable outstanding customer operations while balancing risk, resource constraints and the need for innovation, and that are subject to clear and measurable performance goals for securing information resources and systems Department-wide.
- *Crosscutting Principles*
    1. "One Team, One Fight"
    2. Employment of risk management methodology
    3. Prioritized planning and resourcing
    4. Enterprise-wide collaboration
- *IT Goal 1*: Deliver high quality IT and cybersecurity solutions
    Objective 1.1: Secure and Reliable Information Access
        - Major Tasks
            - Ensure the availability of and access to systems, networks, and information resources that enable DOE to perform the full lifecycle of its mission-essential functions.

- Leverage new network paths and secure data transfer technologies to increase internal and external information flow across DOE sites and operating environments.

Performance Plan

Objective: 2.1 IDENTIFY – Enhance organizational capabilities to manage the cybersecurity risk.

- *Performance Goal (Measure): Hardware Asset Management – Achieve performance of 95% or greater for both Hardware Asset Management metrics (asset detection and asset meta data collection)*

- *Endpoint Target: Annually maintain performance of at least 95% for both Hardware Asset Management metrics by FY 2018 and maintain annually thereafter.*

  - *2019 Target:* ≥ 95 %

  - *2020 Target:* ≥ 95 %

Key Challenges

1. Cybersecurity Preparedness
   - Increasing sophistication and frequency of cyber threats on a growing attack surface.
   - Meeting stringent privacy and security requirements while exchanging data

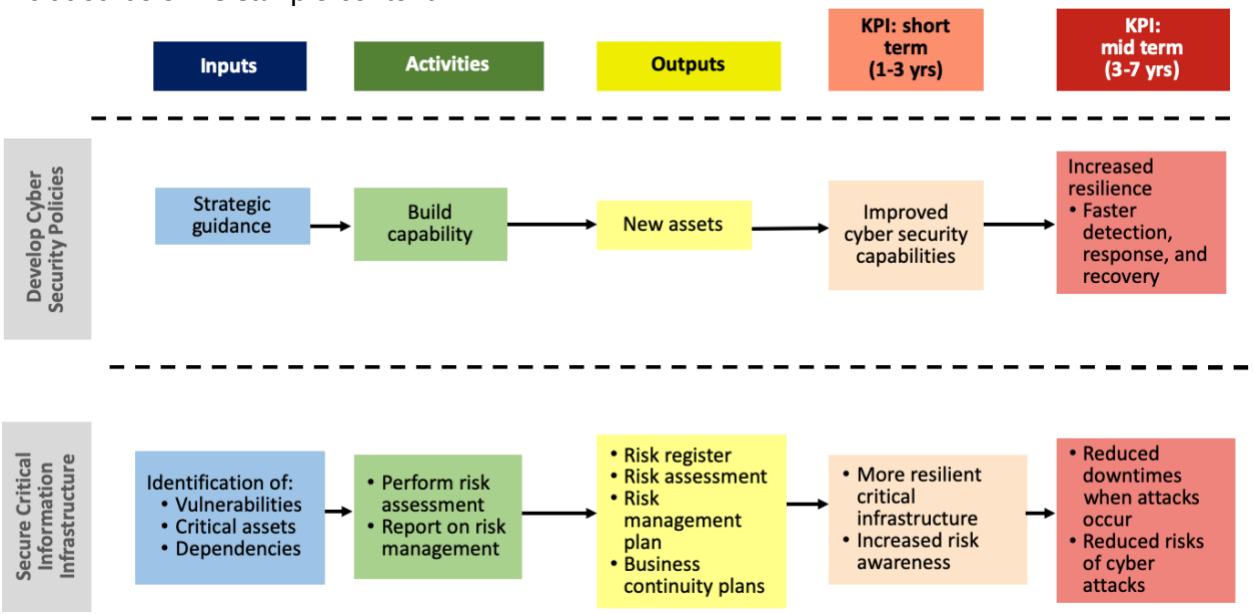
3. Resilient Systems
   - New solutions must support the business case
   - Diverse legacy and modern devices
   - Solutions from diverse vendors and third-party providers must interoperate

3.4 ENISA

The ENISA national cyber security strategies template include the following:

- Vision
- Scope
- Strategic Objectives
    - Roadmap
        - Specific activities to meet the strategic objectives
        - Activities action plan
        - Strategy key performance indicators (KPIs)

Included below is sample content:



4 REFERENCES

1. *How To Build A Strategic Cyber Security Plan,* Posted by Nettitude on Oct 18, 2018 1:22:23 PM, https://blog.nettitude.com/how-to-build-a-strategic-cyber-security-plan

2. ENISA, *An evaluation Framework for National Cyber Security Strategies,* November 2014.

3. ENISA, *NCSS Good Practice Guide - Designing and Implementing National Cyber Security Strategies*, November 2016.

4. U.S. *Department of Energy Cybersecurity Strategy 2018-2020*, June 2018.

5. *U.S. Department of Homeland Security Cybersecurity Strategy*, May 2018.

6. *US Transportation Security Administration Cybersecurity Roadmap, 2018*.

5 ACRONYMS

DHS	US Department of Homeland Security
DOE	US Department of Energy
ENISA	European Union Agency for Network and Information Security
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
TSA	US Transportation Security Administration
US	United States