U.S. DEPARTMENT OF ENERGY

DOE CRITICAL INFRASTRUCTURE CYBERSECURITY FRAMEWORK

SECURING OPERATIONAL TECHNOLOGY AND ENERGY SYSTEMS

ZERO TRUST ARCHITECTURE

OT / ICS PROTECTION

CLOUD & EDGE SECURITY

AI-ASSISTED THREAT DETECTION

SOC MODERNIZATION

DEVSECOPS INTEGRATION

INCIDENT RESPONSE & CONTINUITY

GOVERNANCE & COMPLIANCE

An integrated, risk-based cybersecurity framework designed to protect mission-critical energy infrastructure, enhance threat resilience, and ensure operational continuity across DOE environments.

SECURE OPERATIONS

MISSION RESILIENCE

RISK-BASED DECISIONS

COLLABORATION & ACCOUNTABILITY

CONTINUOUS IMPROVEMENT

PROTECTING TODAY. POWERING TOMORROW.

Table of Contents

Executive Summary

The Department of Energy (DOE) operates and supports some of the nation's most critical infrastructure, including energy distribution systems, Industrial Control Systems (ICS), Operational Technology (OT), and interconnected energy management platforms. As these environments evolve into highly digital and interconnected ecosystems, they face increasingly complex and sophisticated cyber threats that can impact operational continuity, infrastructure resilience, and national security. This framework establishes a comprehensive cybersecurity strategy designed to secure these mission-critical environments while enabling modernization across hybrid, cloud, and distributed operational systems.

The framework integrates key cybersecurity capabilities, including Zero Trust Architecture (ZTA), OT and ICS protection, cloud and edge security, AI-assisted threat detection, SOC modernization, and DevSecOps practices. These capabilities are designed to enhance threat visibility, reduce risk exposure, and improve detection and response across IT and OT domains. By combining advanced security controls with continuous monitoring, telemetry analysis, and coordinated incident response, the framework strengthens the overall cybersecurity posture while supporting secure and scalable infrastructure operations.

Aligned with regulatory standards and mission objectives, the framework emphasizes operational resilience, risk-based decision-making, and compliance-driven governance. It ensures the protection of critical assets while maintaining system availability, safety, and continuity of energy operations. Through this integrated and adaptive approach, DOE can sustain secure, reliable, and resilient energy infrastructure capable of withstanding evolving cyber threats and supporting long-term modernization initiatives.

Critical Infrastructure Threat Landscape

DOE operational environments face an increasingly complex and evolving threat landscape driven by nation-state actors, ransomware campaigns, ICS/SCADA exploitation, supply chain compromises, insider threats, and distributed denial-of-service attacks. The convergence of IT and OT systems has significantly expanded the attack surface, exposing interconnected infrastructure to threats that can disrupt energy delivery, degrade operational visibility, and compromise sensitive data. These risks are amplified in mission-critical environments where system availability and safety are prioritized, making them attractive targets for high-impact cyber operations.

The most significant threat vectors include ransomware and destructive malware targeting operational continuity, exploitation of industrial control systems affecting core processes, and supply chain vulnerabilities introduced through vendors, contractors, and third-party dependencies. These threats can lead to cascading impacts across interconnected systems, affecting not only individual facilities but broader energy infrastructure networks. As operational environments become more digitized and interconnected, adversaries gain more opportunities to exploit weak points across hybrid architectures.

Addressing this threat landscape requires a risk-based cybersecurity approach focused on asset visibility, network segmentation, identity protection, and continuous monitoring across IT and OT domains. Effective mitigation strategies must balance strong security controls with operational requirements, ensuring that threat detection, response, and resilience capabilities are integrated without disrupting critical infrastructure operations. By aligning security measures with evolving threats, DOE can better protect mission-critical systems and sustain reliable energy operations in a high-risk environment.

Framework Objectives

The primary focus is on establishing identity-centric security, reducing attack surface exposure, and enhancing protection across IT, OT, cloud, and edge systems. By implementing Zero Trust principles, including continuous authentication, least-privilege access, and segmentation, the framework aims to limit unauthorized access and prevent lateral movement across interconnected infrastructure.

A key objective is to improve threat detection and response through centralized telemetry aggregation, AI-assisted analytics, and modernized SOC operations. These capabilities enhance visibility into operational environments, enabling faster identification of threats and more effective incident response. In parallel, the framework prioritizes the protection of OT and ICS systems through asset visibility, secure communications, and segmented network architectures, ensuring that critical infrastructure is safeguarded without compromising operational continuity.

The framework also emphasizes secure cloud and edge integration, operational resilience, and compliance alignment with federal standards. This includes implementing secure configurations, continuous monitoring, and structured incident response and recovery strategies to maintain system availability during disruptions. By integrating governance, risk management, and continuous improvement processes, the framework supports long-term cybersecurity maturity while enabling secure modernization and sustained energy operations.

DOE Cybersecurity Operating Environment

The DOE Cybersecurity Operating Environment encompasses a complex and highly distributed ecosystem of Industrial Control Systems (ICS), SCADA platforms, smart grid infrastructure, cloud-hosted analytics, edge computing nodes, and contractor-managed systems. These components operate across hybrid architectures that integrate legacy Operational Technology (OT) with modern IT and cloud-native services, creating interconnected environments that support mission-critical energy operations. This convergence increases system interdependencies and expands the attack surface, requiring cybersecurity approaches that account for diverse trust boundaries, dynamic data flows, and geographically dispersed infrastructure.

The environment is further challenged by the presence of legacy OT and ICS assets that were not designed with modern cybersecurity controls, limiting patching, monitoring, and protection capabilities without risking operational disruption. Additionally, reliance on contractors, vendors, and third-party providers introduces supply chain dependencies and expanded access pathways, increasing exposure to compromise. These factors demand strong identity and access management, strict segmentation, and enhanced oversight of external integrations to mitigate risks across both internal and extended operational ecosystems.

Given these conditions, the DOE operating environment requires a unified cybersecurity architecture that enables real-time visibility, continuous monitoring, and coordinated response across IT, OT, cloud, and edge domains. Security controls must be carefully engineered to balance protection with operational continuity, ensuring that safety-critical processes, system availability, and energy delivery are not disrupted. Effective cybersecurity in this context depends on resilient, interoperable systems that support secure communications, telemetry synchronization, and adaptive risk management across all mission-critical infrastructure layers.

Zero Trust Architecture for DOE Operations

The DOE Zero Trust Architecture (ZTA) establishes an identity-centric security model designed for highly distributed and mission-critical energy environments where traditional perimeter defenses are insufficient. It enforces continuous authentication, least-privilege access, and dynamic trust evaluation across all users, devices, and systems—including federal personnel, contractors, and third-party providers. By treating identity as the primary control plane, ZTA enables consistent enforcement of multi-factor authentication (MFA), role-based access control (RBAC), and adaptive access policies across IT, OT, cloud, and edge environments, reducing unauthorized access and limiting exposure across interconnected infrastructure systems.

At the operational level, Zero Trust is implemented through layered security controls spanning identity, device, network, application, and data domains. Micro-segmentation across IT and OT networks isolates critical systems such as ICS, SCADA, and telemetry platforms, preventing lateral movement and containing potential compromises. Continuous monitoring and telemetry-driven validation enable real-time access decisions based on behavior, device posture, and threat intelligence, ensuring that access permissions are dynamically adjusted according to risk rather than static trust assumptions. This approach enhances visibility and strengthens coordinated threat detection and response capabilities across distributed operational environments.

The architecture is specifically designed to align with the operational constraints of DOE environments, where system availability, safety, and reliability are paramount. Security controls are engineered to integrate with legacy and mission-critical OT systems without disrupting industrial processes, ensuring continuity of energy operations while improving security posture. Additionally, ZTA supports secure interoperability across IT, OT, cloud, and contractor-managed systems through unified policy enforcement and secure communication channels, enabling a resilient and scalable cybersecurity framework that reduces attack surface and supports rapid containment of cyber threats.

Operational Technology (OT) Security Architecture

The Operational Technology (OT) Security Architecture establishes a specialized security model designed to protect Industrial Control Systems (ICS), SCADA platforms, and energy infrastructure operations without disrupting mission-critical processes. It emphasizes segmented network design, secure industrial communications, and controlled interaction between enterprise IT and OT environments to minimize unauthorized access and reduce lateral movement. By enforcing strict boundaries around critical systems such as telemetry platforms and industrial controllers, the architecture strengthens protection of operational processes while maintaining system integrity and reliability.

Central to the architecture is comprehensive visibility and continuous monitoring across OT assets, enabling early detection of anomalies, threats, and operational risks. Secure communication pathways and access controls are implemented to protect data flows between distributed systems while ensuring only authorized entities can interact with sensitive operational components. These controls are complemented by telemetry monitoring and coordinated incident response capabilities, allowing for rapid identification, containment, and mitigation of cybersecurity events across interconnected operational environments.

The architecture is designed to align with the unique constraints of DOE environments, where availability, safety, and system stability are paramount. Security measures prioritize non-disruptive implementation, ensuring that protections do not interfere with industrial processes, automation workflows, or energy delivery operations. By integrating resilience planning, recovery capabilities, and operational continuity considerations, the OT security architecture supports sustained mission operations while enhancing the overall cybersecurity posture of critical infrastructure systems.

Cloud & Edge Security Integration

The Cloud & Edge Security Integration model supports DOE modernization by securing cloud-native platforms, distributed analytics, and edge computing environments that enable real-time operational intelligence and telemetry processing. These environments operate across hybrid infrastructures, requiring consistent security controls aligned with federal standards such as FedRAMP and NIST, as well as DOE-specific operational and compliance requirements. The integration model ensures that cloud and edge systems maintain secure configurations, protected data flows, and reliable interoperability across mission-critical energy operations.

Cloud security is reinforced through secure API integrations, encrypted data synchronization, workload protection mechanisms, and continuous monitoring of cloud-native services. These controls enable visibility into operational activities while safeguarding sensitive data and ensuring compliance with governance standards. In parallel, edge security extends protection to distributed nodes by enabling localized processing, secure telemetry handling, and resilience in communication-constrained environments, reducing latency while maintaining data integrity and system security.

To support operational continuity, the integration framework emphasizes resilience, scalability, and coordinated security across cloud and edge domains. This includes protecting AI-driven analytics, ensuring secure data exchange between centralized and distributed systems, and maintaining continuity of operations during disruptions. By enforcing unified security policies and continuous validation across all environments, the model strengthens DOE’s ability to manage risk, maintain situational awareness, and sustain secure, real-time energy operations across geographically dispersed infrastructure.

AI-Assisted Threat Detection Framework

The AI-Assisted Threat Detection Framework enhances DOE cybersecurity operations by integrating machine learning and advanced analytics into continuous

monitoring and threat identification processes. It leverages aggregated telemetry from IT, OT, cloud, and edge environments to detect anomalous behavior, identify emerging threats, and provide actionable intelligence across mission-critical systems. By correlating real-time and historical data, the framework improves visibility into complex operational environments and strengthens the ability to detect sophisticated attacks targeting interconnected infrastructure.

AI-driven capabilities focus on behavioral analytics, anomaly detection, and predictive threat modeling to identify deviations from normal operational patterns, including insider threats, infrastructure anomalies, and coordinated cyber activities. These models continuously learn from operational data and incident history to refine detection accuracy and prioritize high-risk events. Automated analysis reduces noise from large telemetry volumes, enabling security teams to focus on critical threats while improving response speed and decision-making across distributed environments.

To support rapid response and operational resilience, the framework incorporates automated containment, adaptive access controls, and incident escalation workflows. These capabilities enable dynamic mitigation actions such as restricting access, isolating affected systems, and prioritizing response activities without disrupting critical operations. By integrating AI-driven detection with coordinated response mechanisms, the framework enhances DOE's ability to proactively manage cyber risks, maintain situational awareness, and sustain secure, continuous energy operations.

Security Operations Center (SOC) Modernization

The Security Operations Center (SOC) Modernization initiative enhances DOE cybersecurity capabilities by establishing a centralized and integrated monitoring environment that consolidates telemetry from IT, OT, cloud, and distributed operational systems. Through the integration of SIEM and SOAR platforms, the SOC enables real-time analysis, correlation, and prioritization of security events across mission-critical infrastructure. This centralized approach improves visibility into complex, geographically dispersed environments while enabling faster detection of threats and coordinated response actions.

Modernized SOC operations emphasize automation, intelligence-driven workflows, and cross-domain situational awareness to improve efficiency and reduce response times. Automated orchestration supports incident triage, threat containment, and escalation processes, allowing security teams to focus on high-impact threats while maintaining continuous monitoring across contractor-managed and operational environments. This model also strengthens collaboration between security, operational,

and incident response teams, ensuring a unified approach to managing cybersecurity risks.

To support resilience and operational continuity, the SOC framework integrates coordinated incident response, recovery planning, and infrastructure-wide monitoring capabilities. It enables rapid containment of threats while preserving system availability and operational stability across energy environments. By aligning advanced monitoring, automation, and response coordination, the modernized SOC enhances DOE's ability to maintain situational awareness, mitigate cyber risks, and sustain secure, uninterrupted mission-critical operations.

DevSecOps Security Integration

The DevSecOps Security Integration model embeds cybersecurity controls directly into the software development and deployment lifecycle, ensuring that security is continuously enforced across DOE operational environments. By integrating automated security testing, continuous integration and continuous deployment (CI/CD) pipelines, and infrastructure-as-code (IaC) validation, the framework enables secure and efficient delivery of applications and services supporting mission-critical energy systems. This approach reduces vulnerabilities early in the development process and ensures that modernization efforts remain aligned with cybersecurity and compliance requirements.

Security capabilities within DevSecOps include automated vulnerability scanning, configuration validation, policy-as-code enforcement, and runtime compliance monitoring across cloud-native and hybrid infrastructures. These controls provide consistent oversight of system configurations and application behavior, ensuring that both new and existing deployments adhere to established security standards. Continuous monitoring and automated remediation workflows further enhance the ability to detect and address risks in real time, improving resilience across distributed IT, OT, and cloud environments.

By integrating security into every phase of development and operations, the framework strengthens collaboration between development, security, and operations teams while maintaining operational agility. This unified approach supports secure modernization initiatives, reduces deployment risks, and ensures that DOE systems remain resilient, compliant, and protected against evolving cyber threats without disrupting critical energy operations.

Incident Response & Operational Continuity

The Incident Response and Operational Continuity framework establishes a structured and resilient approach to managing cybersecurity events across DOE operational environments. It prioritizes rapid threat detection, containment, and coordinated response to minimize disruption to mission-critical energy systems. By integrating predefined response procedures, escalation protocols, and cross-functional coordination, the framework ensures that cybersecurity incidents are addressed efficiently while maintaining visibility across IT, OT, cloud, and distributed infrastructure systems.

The framework incorporates comprehensive continuity planning, including failover strategies, backup and recovery capabilities, and telemetry preservation to support sustained operations during and after cyber incidents. These capabilities are designed to maintain system availability and protect critical processes, ensuring that energy production, distribution, and research activities continue despite disruptions. Regular testing and validation of recovery procedures further strengthen resilience and readiness across operational environments.

To support long-term operational stability, the model emphasizes coordinated incident management, real-time monitoring, and adaptive response mechanisms that align with the unique constraints of DOE systems. This includes preserving safety-critical functions and minimizing impact on industrial processes while enabling rapid restoration of services. By aligning incident response with operational continuity objectives, the framework enhances DOE’s ability to sustain secure, reliable, and uninterrupted energy operations in the face of evolving cyber threats.

Governance & Compliance Framework

The Governance & Compliance Framework establishes a structured approach to managing cybersecurity oversight, risk management, and regulatory alignment across DOE operational environments. It aligns cybersecurity practices with federal standards and directives, including NIST, FedRAMP, and DOE-specific requirements, ensuring that security controls are consistently implemented across IT, OT, cloud, and contractor-managed systems. This alignment supports a standardized security posture while enabling risk-based decision-making tailored to mission-critical energy operations.

The framework defines clear governance structures, including executive oversight, operational security teams, and specialized OT governance functions responsible for policy enforcement, risk assessment, and compliance validation. Continuous compliance monitoring and audit mechanisms are integrated to assess adherence to security

standards, identify control gaps, and prioritize remediation efforts. These processes enable proactive management of cybersecurity risks while maintaining accountability and transparency across distributed operational environments.

To support long-term resilience and modernization, the framework incorporates risk-based prioritization, continuous improvement processes, and alignment with evolving federal cybersecurity mandates. By integrating governance with operational security practices, it ensures that cybersecurity initiatives remain adaptable, compliant, and aligned with mission objectives, strengthening DOE's ability to sustain secure, resilient, and compliant infrastructure operations in an evolving threat landscape.

Performance Metrics & Operational KPIs

The Performance Metrics & Operational KPIs framework establishes a structured approach for measuring cybersecurity effectiveness, operational resilience, and modernization progress across DOE environments. It defines quantifiable indicators that provide visibility into system performance, threat detection capabilities, and overall security posture across IT, OT, cloud, and distributed operational systems. These metrics enable informed decision-making by linking cybersecurity performance with mission-critical objectives such as system availability, infrastructure reliability, and risk reduction.

Key performance indicators focus on areas such as incident frequency, mean time to detect and recover (MTTR), OT system availability, vulnerability remediation timelines, telemetry coverage, and compliance validation rates. Additional metrics assess the effectiveness of AI-assisted threat detection, network segmentation maturity, and response efficiency across interconnected environments. Together, these KPIs provide a comprehensive view of operational security, helping identify gaps, prioritize remediation, and strengthen visibility into evolving cyber risks.

To support continuous improvement, the framework emphasizes ongoing monitoring, performance benchmarking, and alignment with governance and compliance objectives. Metrics are used to evaluate the effectiveness of security controls, guide resource allocation, and track progress toward cybersecurity maturity goals. By integrating performance measurement with operational oversight, the framework enables DOE to sustain resilient, data-driven cybersecurity operations while ensuring alignment with mission priorities and evolving threat conditions.

Future-State Cybersecurity Vision

The Future-State Cybersecurity Vision for DOE operational environments centers on the evolution toward intelligent, adaptive, and highly resilient security ecosystems capable of supporting increasingly digital and interconnected energy infrastructures. As environments expand across cloud-native platforms, edge computing, and distributed telemetry systems, cybersecurity capabilities must evolve to provide continuous, real-time protection and visibility across all operational domains. This vision emphasizes the integration of advanced analytics, automation, and scalable architectures to secure mission-critical operations while enabling modernization and innovation.

A key component of the future state is the adoption of AI-driven and predictive cybersecurity capabilities that enhance threat detection, risk analysis, and incident response. These capabilities leverage large-scale telemetry, behavioral modeling, and automated decision-making to identify emerging threats and proactively mitigate risks before they impact operations. In parallel, the environment will support secure interoperability across IT, OT, cloud, and contractor-managed systems, ensuring consistent policy enforcement, data protection, and coordinated defense across highly distributed infrastructure.

Ultimately, the future-state vision extends beyond traditional cybersecurity by establishing a unified, resilient, and intelligent defense framework aligned with mission-critical energy objectives. It prioritizes adaptive protection, autonomous monitoring, and continuous improvement to ensure long-term operational stability and security. By aligning cybersecurity innovation with infrastructure resilience and operational continuity, DOE can sustain secure, reliable, and forward-looking energy operations in an increasingly complex threat landscape.

Conclusion

The DOE Critical Infrastructure Cybersecurity Framework establishes a comprehensive cybersecurity modernization strategy supporting operational continuity, infrastructure resilience, cloud modernization, AI integration, and evolving cyber threat protection across mission-critical energy environments.

By integrating Zero Trust Architecture, OT and ICS cybersecurity, cloud-native security controls, AI-assisted monitoring, DevSecOps methodologies, operational resilience planning, and compliance-aligned governance, the framework provides a strategic roadmap for securing distributed energy ecosystems while supporting modernization initiatives and long-term national energy resilience.