**Energy Sector: Cyber Risk & Resilience Framework Outline**

**Executive Summary:**

**Due to current system innovations and the scope of services the Electric Sector provides, the Electric Sector and its architectures face significant cyber threats from a broad range of highly sophisticated actors.** The Electric Sector entities vary in size, which can cause inequities in technological and financial resources, creating disparities in staff expertise and funding. Current best practices to identify cybersecurity vulnerabilities and gaps and implement best practices are understandably NIST Framework, ISSO, C2M2, CMMC and compliance based, which are foundational but not sufficient. While Electric Sector entities are cognizant of current cyber threat actors and methods, many do not know how to expeditiously identify, prioritize, and effectively mitigate their top cyber risks versus primarily responding to standards-based audits.

With the advent of and access to broad network & Industrial Control Systems (ICS) data sets, Artificial Intelligence (AI) driven analytics, and instrumentation, there are now commercial grade IT, Operational Technology (OT), and ICS risk rating capabilities that can be leveraged externally and internally, providing effective transparency, risk monitoring, and mitigation. By providing affordable access to best-of-breed continuous risk monitoring, prioritization, and mitigation services Electric Sector-wide, a majority of risks can be affordably identified and addressed.

**A1.** What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

States, Local, and Tribal units of government can be enabled and supported by Cyber Risk Platforms as a Service being made available from the Federal level. Having developed such a commercial platform ( <https://www.whitehawk.com/cyber-risk-paas>) and being the lead developer for the DHS CISA QSMO Cybersecurity Marketplace program*(* [*https://www.cisa.gov/cyber-qsmo-services*](https://www.cisa.gov/cyber-qsmo-services)*),* WhiteHawk knows first-hand the impact of making a cyber risk ecosystem available and accessible. We do this across a Critical Infrastructure Sector in near real time, to include risk monitoring, maturity, risk prioritization, and Blue Teaming with mapping to vetted and proven solution options. Using our approach, all IT/Cyber Suppliers/Vendors/Contractors are vetted and enabled to be CMMC compliant, and all software solutions are vetted, tested, and monitored continuously, providing secure software and hardware asset management and resilience at scale. Our solution drives the State, Local, and Tribal Energy Entities beyond Authority to Operate (ATO)/Authority to Proceed (ATP) and incorporates Cyber Supply Chain Risk Management (C-SCRM).

**A2.** What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

This critical Energy Sector need can be cost effectively met at scale by establishing an accessible C-SCRM Service of Common Concern, available to all via next generation C-SCRM platforms like WhiteHawk's Cyber Risk Radar. We provide details at <https://www.whitehawk.com/cyber-risk-radar>.

**A3**. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector?

Continuous vetting of next generation, OT/ICS/IT/Cyber technologies and making them available via an open Energy Sector online Marketplace can drive performance, assurance, and resilience excellence. We include an example at <https://www.whitehawk.com/innovative-vendors> which could be run by an Energy Sector non-profit, a Federally Funded Research and Development Center (FFRDC), or a University Affiliated Research Center (UARC). What are the potential costs and benefits of those actions? Vice having all Public Entities or Private Companies doing the vetting, testing, and assessments individually, a consortium approach that is openly made available via an Energy Sector wide online Marketplace, for example <https://www.whitehawk.com/marketplace/products>, saves the entire Energy Sector Industry duplicative efforts and tens of millions of dollars annually.

All of the below questions could be continuously and seamlessly addressed with a “Service of Common Concern” approach to:

1. U.S. Energy Sector Risk Management Framework - Outside-in, “Hacker View” OT/ICS/IT risk monitoring, alerting, trend analytics and automated Cyber Risk Baselines, Scorecards and Baselines as illustrated here:
2. [Cyber Risk and Vulnerability Trend Analysis of the U.S Energy Sector](https://communications.whitehawk.com/WhiteHawk-products-services/Cyber-Risk-and-Vulnerability-Trend-Analysis-of-the-US-Energy-Sector.pdf) and here: <https://www.whitehawk.com/cyber-risk-scorecard> U.S. Energy Sector SCRM & C-SCRM Framework - Continuous risk monitoring of both business and cyber risks of Energy Sector OT/ICS/IT via an integrated and assessable Vendor Risk Management (VRM) Dashboard and platform: <https://www.whitehawk.com/cyber-risk-radar>

**A4.** Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

The Department, in coordination with the Department of Electricity, could issue guidance that focuses on review and identification of threat risks associated with hostile nation states. Using threat data from across the sector would enable early identification of risks to critical systems and foreign influence concerns. Using sector-wide analytics, the Department could require testing criteria for critical components with foreign influence. This could be combined with requirements to establish incident response plans and continuity of operations plans for operations with a foreign influenced critical component.

**B1.** To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, *i.e.,* distribution equipment and facilities?

The Department should consider implementing a risk-based approach to assessing a Prohibition Order. The focus of the assessment would address the systems that could have a widespread impact across the distribution infrastructure or significant impact on critical sectors. The Department should consider an approach similar to the Department of Defense (DoD) criteria in Section 889, of the Federal Acquisition Regulations (FAR).

**B2.** In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems?

As an alternative to prohibitive orders that would be compliance-based, the Department could consider a strategy of investment, incentivization, and modernization that would better secure these critical sectors. These incentives would prioritize implementation of rigorous independent testing and security as a core business function rather than compliance to slow changing procurement requirements not associated with evolving threats. Implementation of these testing and security-based metrics could be monitored and supported by an independent entity such as a non-profit FFRDC or UARC using a C-SCRM “Services of Common Concern” approach and a ready marketplace for acquiring tested and vetted security solutions.

**B3.** In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure enabling the national critical functions?

A prohibitive order of this magnitude would not be practical without being highly disruptive. Many of the utilities do not have the ability to identify the critical infrastructure within their territories, and the distributed nature of the infrastructure could result in the entire infrastructure falling under this order. Additionally, the expense of replacing prohibited equipment would be costly without having any guarantee of increasing the security of the nation’s infrastructure. An alternative risk and threat-oriented approach of investment, incentives, and modernization based on the “Services of Common Concern” would serve to focus threat testing and evaluation on the most critical risk-based threats. With sector-wide threat focused analysis, domestic manufacturers could be incentivized to manufacture secure trusted solutions for the most needed and critical parts to protect against foreign influenced threats. This approach, coupled with incentivized security-based modernization efforts, would enable all electrical providers to cost effectively address security as a function of their core business processes while transitioning to domestic suppliers with tested and trusted components.

**B4.** Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements?

Please see the response to question B3.

**A. Development of a Long-Term Strategy**

 The Energy Sector and its multiple architectures face a relentless cyber threat from a broad range of sophisticated actors. The 3,400+ energy companies and entities vary greatly in size, cybersecurity expertise, and financial resources, creating great disparities in staff expertise and available funding. Commissioners and Executives are aware of the general cyber risks impacting their Sector, but do not have continuous insight into current cyber risk indicators, capability gaps, and threat trends across their region, company ecosystem, or supply chain. Therefore, today’s focus is primarily on implementing best practices and known standards, all of which is foundational but not sufficient, to ensure sector-wide resilience and performance through any major cyber event.

 A Cyber Risk Management Framework, with a “Hacker View” continuous monitoring, alerting, trend reporting, gap analysis, and executive level discussion points can inform Energy Sector stakeholders of the current Cyber Risk Posture for each entity/company; risk trends by sub-sector, region, and size; and how to continuously identify and mitigate their priority risks smartly and affordably. The development of a National Cyber Risk Management program for the Energy Sector can drive the achievement of three key objectives:

 1. Strengthening energy sector Digital Age preparedness,

 2. Coordinating cyber incident response and recovery, and

 3. Accelerating research, development, and demonstration (RD&D) of game-changing and resilient energy delivery systems.

The first two strategic efforts are building the energy sector’s day-to-day operational capabilities to have continuous insight into shared risks and key vulnerabilities, improve organizational and process level cyber maturity, and efficiently perform cyber-incident response and recovery. Knowing the current Energy Sector Threat Landscape is foundational to this – and it should not be limited to self-reported known incidents but include an outside-in, “Hacker View” of risk.

 To achieve these critical objectives, the Department of Energy (DOE) and Department of Electricity should fully leverage The Office of Cybersecurity, Energy, Security, and Emergency Response (CESER) or DOE CIO JC2 to manage the continuous identification and prioritization of cyber threat and risk trends across the Energy Sector, mapping those capability gaps to best practices and next generation solutions that achieve an acceptable level of security and resilience. This requires that DOE’s designated organization determines and prioritizes key cyber risk scenarios and response and recovery requirements while also identifying cost effective solutions that can scale from small municipal providers to multi-state enterprises. In addition, the Department of Electricity needs to establish consistent resilience criteria and reporting metrics based on evolving threat vectors and technologies. This assessment and prioritization of key cyber risk scenarios can be mapped to RD&D requirement objectives enabling the development of innovative cyber-resilient energy infrastructure through the RD&D of new tools and technologies to reduce the risk that energy production and delivery might be disrupted by a cyber incident. WhiteHawk recommends the following goals, objectives, and methods In developing a long-term strategy for the Department of Electricity.

**Goals:**

* Establish an Energy Sector Cyber Risk & Resilience Management Framework
* Baseline the Sector’s current Cyber Risk Posture down to the entity level
* Map Initiatives to Address Priority Risks (Policies, Best Practices, Training, Technical)
* Share on a quarterly basis with Key Stakeholder Executives & Regulators sector-wide

**Objectives:**

* Continuous Cyber Risk Monitoring, Alerting, and Scoring of Cyber Risk Indicators across the Energy Sector, by sub-sector, by region, and down to the entity level (including all 3,400+ Private and Public Sector Energy Entities)
* Detailed analysis and reporting of cyber risk trends by Energy Sub-Sector and Region
* Identification and tracking of priority cyber vulnerabilities and gaps across all Energy Sub-Sectors and Regions
* Integrated Software as a Service (SaaS) Dashboard and Portal access and insights into risk ratings and risk mitigation in real-time
* Creation and Tailoring of Executive Level Reporting of Trends, Measures, and Metrics to DOE CESER needs
* Foundational trend analysis and key gap overviews mapped to potential policy, standard, and technology recommendations and initiatives
* Development of consistent measures and metrics of cyber risk mitigation, maturity levels, and continuous improvement

**Methods:**

Monitor, identify, and track priority cyber vulnerabilities and gaps. Leverage AI-based risk platforms and advanced SaaS partners to identify, prioritize, and mitigate cyber risks impacting the revenue, reputation, and operations of the Energy Sector.

Phase I: Visualize some of the key risk indicator trends by entity size, on a subset of data across the Energy Sector. Each top trend is paired with a best practice or solution. Start with cyber risk monitoring and prioritization of risk indicators going back one year:

* Know the sector’s threat landscape and vector trends
* Receive Executive Level Cyber Risk Scorecard summation report on a quarterly basis (Example included at Attachment A)
* Leverage a real-time Red Team Assessment to validate all discovered & Sector-wide risks
* Conduct Dark Net Assessment of obfuscated IP addresses & lost data sets
* Identify vetted, best-of-breed solution options to mitigate all validated cyber risks
* Be accountable to Leadership and Stakeholders, leveraged by the CIO/CISO/IT Team
* Ensure global reach, while tailoring and scaling to any size organization or company



Phase II: Identify additional macro level trends of cyber risk issues identified within specific segments of Energy Sector monitored companies. Annually or semi-annually, integrate cutting edge SaaS based Red Team assessments:

* Validate and prioritize Cyber Risk Scorecard key risk indicators
* Stay up to date on hacker intentions, methods, and tools
* Track major attack methods and impacts they are having globally –across all Sectors
* Compliment inside Red Team limited findings
* Determine where to focus your limited resources

Phase III:Have amatrix is developed showing high level trends from, for example, WhiteHawk’s deep dive analysis of representative samples of the Energy Sector’s Small, Medium, and Large Enterprises. Following this path will produce Cyber Risk Scorecards designed to provide entities with actionable information to:

* Enable budget-based, effective risk reduction decision making
* Facilitate smart and timely action
* Prevent online crime and fraud from disrupting operations
* Affordable and impactful options to mitigate key cyber risks

**Enabling Better Testing of Critical Grid Equipment**

WhiteHawk continuously vets innovative, game-changing, scalable, and cost-effective cybersecurity solutions (over 1,500 to date) in order to address any category of Digital Age Risk. Our continuous research enables us to provide expert-vetted risk mitigation solutions tailored to the enterprise’s needs. What we have discovered through this process is that solutions exist for many of the problems concerning testing and cybersecurity, but organizations are unwilling to invest in these solutions without a compelling requirement.

For most manufactures and consumers of Critical Grid Equipment, cybersecurity testing is an imposed cost for which they perceive little to no return on investment. This is especially true of small to mid-sized companies where cybersecurity risks are not well defined and the cost of securing the infrastructure from all threats would be prohibitive. To better enable these small to mid-sized companies’ efforts to test and secure critical components, DOE should consider models that distribute the cost of this testing while leveraging sector analytics to focus testing on the areas of greatest risk. Establishing an analysis clearing house, similar to an Underwriters Laboratories or the Energy ISAC will help enable this effort.

**Objectives:**

* Deliver affordable and impactful options to mitigate cyber risks of small and midsize businesses and organizations, prioritized to reduce the most significant risks.
* Collect, analyze, and correlate openly available data into actionable intelligence.

**Methods:**

In the Digital Age environment, hardware, software, solutions, and services interconnect at many levels to Private and Public Sector capabilities, platforms, and missions. Our economic, political adversaries and criminals continuously seek to steal, disrupt, and conduct industrial espionage against all that they can, gaining and holding root-level access across critical government systems and their suppliers. A proven external and internal Cyber Risk Assessment program similar to WhiteHawk's is designed and optimized to ensure:

* The entity knows “The Truth About Your Cyber Resilience”
* Questions and tests the entity's Risk Assumptions continuously
* Provides a “High-End Hacker-View” across a Department’s infrastructure, operations, and mission sets
* Implementation of an independent, expert, risk assessment and mitigation strategy from an innovative risk team, using best-of-breed technologies and a truth to power approach tailored to the Department’s Leadership, Managers, and OMB reporting requirements

DOE should leverage open source and industry-specific risk trends and threat data to conduct focused analytics into critical grid equipment. This specific level of focus will allow industry to cost effectively test and secure these risk areas without having to test and secure the entire infrastructure. Industry can then perform deep dives in the areas that need focus rather than into the entire dataset.



**Encouraging Advanced Procurement and Risk Management Practices:**

DOE should enable resilience by encouraging improved procurement practices, informed by risk management practices. Through contracting and purchasing agreements, DOE should weigh vendor selection criteria related to meeting cyber risk trends and reporting requirements. These requirements should be based on the detailed analysis and reporting of cyber risk trends and evaluation of the vendor’s ability to develop consistent measures and metricsof cyber risk mitigation, maturity levels, and continuous improvement.

Compliance should be mapped to solutions to help close vulnerability gaps, validate current posture and document how vendors are meeting controls or achieving compliance. Implementing this process should include the creation and tailoring of Leadership Level Trend Reporting, including measures and metrics, to DOE, and an integrated SaaS Dashboard. Leadership Level Trend Reporting should gather and analyze cyber risk data and analytic outputs for each ‘supplier/vendor’ in the company’s portfolio. Data collection, assessment, and analytics is performed using externally available open data. Ecosystem Maps allow industry to visualize the enterprise by understanding supplier and vendor interconnections and provide industry-wide visibility into threats and mitigation strategies that enable development of cost-effective solutions that can be implemented across the sector.

**Objectives:**

* Gather and analyze cyber risk data & analytic outputs for each ‘supplier/vendor’ in the company’s portfolio
* Perform data collection, assessment, & analytics using externally available open data
* Summary of top findings for prioritization & action
* Report of top risk vectors mapped to best practices & solution options
* Prioritized risk mitigation resourcing strategies

**Methods:**

Summary of top-findings for prioritization and action:

* + Continuous monitoring of control measures linked to NIST Cybersecurity Frameworks and other frameworks (NIST 800-53, NIST 800-171, HIPPA, CMMC, ISO, etc.) for FISMA compliance
	+ Risk Categorization compliance requirements for FIPS 199 (Confidentiality, Integrity, Availability, and Impact)

Report of top risk vectors mapped to best practices & solution options:

* + Risks identified by category and severity with mitigation recommendations
	+ Risks linked to compliance frameworks to understand overall impact to compliance and security

Prioritized risk mitigation resourcing strategies:

* WhiteHawk designed the Cyber Risk Scorecard to provide clients with actionable information to:
* Facilitate budget-based and impactful, risk reduction decision making based upon cyber risk vector indicators
* Enable smart and timely action
* Prevent online crime and fraud from disrupting operations
* WhiteHawk Cyber Analysts perform customized analytics to:
* Deliver affordable and impactful options to mitigate cyber risks of small and midsize businesses and organizations, prioritized to reduce the most significant risks
* Track key actions and mitigations to accept or address known risks
* Provide maturity planning in the form of an achievable risk reduction roadmap, enabling data-driven decision making in terms of business risk and budget constraints
* Maintain informed and enable engagement

Integration into One Vendor Risk Management Dashboard:

* Continuous situational awareness, tracking, mitigation, and management of the Supply Chain Risk Management (SCRM)/Vendor Relationship Management (VRM) program.

**Developing a Strong Domestic Manufacturing Base with High Levels of Security and Resilience**

Development of a strong, secure, and resilient domestic manufacturing base requires consistent targeted incentives that extend beyond voluntary measures existing to date under DOE and FERC programs. While these programs should be expanded, they lack the specificity and focus required to address the most critical vulnerabilities in a timely and cost-effective manner. Additionally, under the current framework, each company is responsible for testing and securing its own infrastructure forcing multiple companies to pay to test and evaluate the same common sets of core infrastructure.

To mitigate these, DOE should employ a commercial testing approach similar to Underwriters Laboratories or Consumer Reports. This model, which could be run by DOE and/or an independent body such as the E-ISAC, could prioritize the testing and validation of domestically manufactured products. Linking this testing to the critical areas of risk identified by sector analytics and threat data would enable domestic producers to identify and develop solutions with the greatest impact, shortening the time to transition these areas away from foreign-based manufacturers.

**Objectives:**

* Provide incentives for Domestic Manufacturing Base to develop the required solutions that improve the security and resiliency of the US power grid
* Leverage sector and industry analytics to ensure that domestic manufacturers are focused on the most critical risk areas associated with the utilization of foreign manufactured infrastructure and equipment
* Utilize cost effective methods for testing the security and resiliency of components and equipment enabling identification and continuous monitoring of trusted suppliers

**Methods:**

* Tax incentives linked to development and production of equipment and components critical to the security and resiliency of the US Power Grid
* Continue FERC [E-2-RM21-3-000](https://www.ferc.gov/media/e-2-rm21-3-000)
	+ Voluntary incentive program, reimbursing or crediting enterprises for cybersecurity investments/upgrades meeting or going beyond minimums
	+ Consider making this compulsory; enterprises should be required to make upgrades but receive a level of reimbursement for upgrades
* [CESER](https://www.energy.gov/ceser/state-local-tribal-and-territorial-sltt-program) has an SLTT Program
	+ Needs to be more direct, most likely in the form of funding/grants
	+ National Association of State Energy Officials (NASEO)
		- 2020 [report](https://www.naseo.org/data/sites/1/documents/publications/Final%20NASEO_Cybersecurity%20Report%20%28062020%29.pdf) has an Action List that could identify critical priorities for funding
	+ [E-ISAC](https://www.eisac.com/services/cyber-security-depth) Involvement
		- Cooperative and Commercial Testing repository
		- Threat Sharing
		- Coordinating body
* Compulsory reporting of cyber incidents – reporting enables more data collection, further improving the ability to take smart action against threats and cyber risks

**Mitigating Risks Associated with Potentially Compromised Grid Equipment Already Installed on the System**

**Objectives:**

* Identify the components, software, and systems which have the greatest potential for impact if compromised
* Leverage threat analytics to assess and prioritize testing and analysis of critical or high-risk equipment based on impact, source, and probability of exploitation
* Validate risks with Red Teaming and penetration testing to close or mitigate those risks which can be exploited
* Support transition from reactive remediation to predictive security maintenance and continuous monitoring practices
* Develop Plan of Action for closing security gaps and implementing a more resilient infrastructure

**Methods:**

DOE should utilize continuous monitoring of power producers and critical manufactures in their supply chain and maintain and share Cyber Risk Portfolio Reporting containing:

* Analytic summaries across the entire supplier portfolio
* Summary of top findings for prioritization & action
* Report of all suppliers/vendors: security rating scores and top risk vectors

**B. Prohibition Authority**

DOE should consider requiring Energy Sector enterprises to use the same prohibitive approach outlined in the 2019 National Defense Authorization Act. The 2019 NDAA includes Section 889, which prohibits the federal government, government contractors, as well as grant and loan recipients from using or procuring products (referred to as covered technologies) from adversarial nations, including several Chinese telecommunications hardware, software, and services companies. There are two specific parts to Section 889 that were implemented in phases.

* Part A, which was implemented first, requires the federal government to not procure, extend, obtain, or renew contracts where covered technologies are present.
* Part B goes further, implying that the government cannot do business with an entity that “uses any equipment, system, or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.”

Part B remains vague and requires regulatory entities to weigh in over the definition the word “uses”, implying that an entity’s supply chain is also subject to the prohibition. Implementation of Section 889 (a)(1)(B) is ongoing. The Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) issued an interim rule amending the Federal Acquisition Regulation (FAR) to implement Section 889. A prohibitive authority in the procurement process ensures supply chain integrity.

Attachment A: Example Cyber Risk Scorecard In-Depth - Colonial Pipeline; automated cyber risk identification, prioritization, maturity model baseline, FAIR Model and action plan report generated from publicly available threat trend and risk global data sets and AI based risk analytics.

**Terry Roberts**

Founder, President & CEO

WhiteHawk Inc.

CyberSecurity Exchange

[www.whitehawk.com](http://www.whitehawk.com/)

 

Our new address is:

[515 King Street, Suite 450](https://goo.gl/maps/J6GsMggjYZfCPLF7A)

[Alexandria, VA 22314](https://goo.gl/maps/J6GsMggjYZfCPLF7A)