Lessons Learned from Reviewing Energy Sector Cybersecurity Plans

A. David McKinnon, Paul Francik, Amy Pollom, Richard Griswold
Pacific Northwest National Laboratory
Richland, Washington, USA
david.mckinnon | paul.francik | amy.pollom | richard.griswold @pnnl.gov

***Abstract*—Cybersecurity planning is foundational to safeguarding critical energy systems. This paper shares key insights derived from the examination of cybersecurity plans submitted by 74 projects to the U.S. Department of Energy's Grid Resilience and Innovation Partnership program. Pacific Northwest National Laboratory staff developed summary statistics and conducted correlation analyses to understand the relationship between various plan attributes and their acceptance status. For example, questions were explored, such as whether plan length or readability impacted the acceptance status of reviewed plans.**

Findings revealed that while certain factors, such as content clarity and adherence to structured guidelines, played a crucial role, others (e.g., sheer length of the document) had minimal influence. This paper also highlights lessons learned and best practices for enhancing the quality and acceptance rates of cybersecurity plans. This work underscores the importance of refining methodologies to develop efficient and impactful cybersecurity plans.

***Index Terms*—Computer Security, Cyber Physical Systems, Electricity Supply Industry, Security Management, System Resilience.**

I. Introduction

Grid operations are transforming in today's interconnected and digitized infrastructure where energy security and cybersecurity are fundamentally inseparable. The resilience, reliability, and safety of energy systems hinge on the strength of the cybersecurity measures implemented to protect them. A comprehensive cybersecurity plan is a key component of a robust cybersecurity program. The plan is both a prioritized list of what an organization should do, as well as a key communication tool that informs project staff of their cybersecurity roles and expectations. Cybersecurity plans should evolve and be updated throughout the lifecycle of a project to account for changes in technology and emerging challenges. Additionally, as mature cybersecurity programs emphasize continuous improvement, efforts should be made to refine and enhance these plans, so they maintain relevance over time and accurately reflect the systems in operation.

The U.S. Infrastructure Investment and Jobs Act of 2021 required projects in the energy sector to submit cybersecurity plans to the U.S. Department of Energy (DOE). DOE offices funded a variety of projects that spanned low, medium, and high risks. Of these, a large cohort of cybersecurity plans were submitted to the Grid Resilience and Innovation Partnership (GRIP) program at the DOE Grid Deployment Office (GDO). Cybersecurity subject matter experts at the Pacific Northwest National Laboratory (PNNL) reviewed these plans against criteria set by DOE's Cybersecurity, Energy Security, and Emergency Response (CESER) office. This paper presents an objective analysis of the strengths, weaknesses, and areas for improvement observed in the cybersecurity plans submitted by 74 projects across two phases of the GRIP program – GRIP-1, projects selected in 2023, and GRIP-2, projects selected in 2024. By identifying recurring challenges and highlighting opportunities where enhanced education and training could drive meaningful progress, this paper aims to provide actionable insights for improving the resiliency and security posture of energy systems and creating tools and processes that help make plans both actionable and informative. Ultimately, the findings and recommendations outlined seek to contribute to the broader goal of strengthening the cybersecurity frameworks that underpin the energy sector's resilience and operational reliability.

This paper is organized as follows: Section 2 introduces the cybersecurity plan requirements, section 3 summarizes the status of the plans, section 4 presents general observations of the plans, section 5 presents quantifiable observations of the plans, and section 6 summarizes the findings.

II. Cybersecurity Plan Requirements

A. Basis of the Cybersecurity Plan Template

The Cybersecurity Capability Maturity Model (C2M2) served as a foundational guide for the development of the high-risk cybersecurity template used by GRIP project participants. Initially developed in 2012 [1], the C2M2 was a collaborative effort between DOE and energy and cybersecurity industry experts as part of a White House initiative to enhance the security posture of the electricity sector. Over the years, hundreds of energy sector stakeholders have contributed to the

The Pacific Northwest National Laboratory is operated by the Battelle Memorial Institute for the U.S. Department of Energy under contact DEAC05-76RL01830.

model's updates, ensuring its ongoing relevance and applicability to evolving cybersecurity challenges [2].

At its core, C2M2 provides a robust framework with more than 350 cybersecurity practices that are grouped into 10 logical domains, each designed to support organizations in assessing and improving their cybersecurity posture. These domains include: Asset Change and Configuration Management, Cybersecurity Architecture, Cybersecurity Program Management, Event and Incident Response, Continuity of Operations, Identity and Access Management, Information Sharing and Communications, Risk Management, Situational Awareness, Third-Party Risk Management, and Threat and Vulnerability Management [3].

Within each domain, cybersecurity practices are organized into actionable objectives, which can be achieved by implementing the practices. For instance, in the Risk Management domain, five key objectives guide organizations in building a robust cyber risk management strategy: establishing and maintaining a cyber risk management program, identifying cyber risks, analyzing risks, responding effectively, and conducting management activities to monitor and reassess risk.

Using the C2M2 as a foundational resource, CESER was able to develop a high-risk IIJA GRIP cybersecurity template tailored to the evolving needs of the energy sector. [4] The CESER template leverages the structured approach of C2M2, using many of the same domains, providing a clear roadmap for energy organizations to enhance cybersecurity resilience while addressing advanced threats in the high-risk energy landscape.

B. Lifecycle of a Cybersecurity Plan

One of the key elements of C2M2 is that it is a maturity model – meaning organizations are expected to mature over time, and they can come back to the model to re-analyze where they have matured and improved their cybersecurity coverage. No organization is expected to achieve 100% coverage or maturation in all areas from the very beginning. It often takes time, training, and often trial and error. Even then resources may constrain coverage that you would like to have but cannot afford. The same can be said for building cybersecurity plans. They evolve over time and closely follow the lifecycle of a project and are expected to mature over time in alignment with the project phases. Cybersecurity plans are living documents that are updated whenever any significant change occurs.

Creating effective and actionable cybersecurity plans is an iterative process that evolves over the lifecycle of a project. This approach emphasizes the importance of progressively developing and refining plans to address the unique context and challenges of each project stage.

The process begins with the design phase, where high-level objectives, assumptions, requirements, and initial risks are identified. This phase serves as the foundation for the cybersecurity plan, focusing on aligning strategies with organizational requirements, industry standards, and anticipated security challenges such as known threats and vulnerabilities. A majority of the submitted plans serve as a prime example of the importance and effectiveness of iterative planning in cybersecurity. Some projects were initially given a pre-award acceptable status, indicating they were demonstrating compliance with the fundamental requirements laid out by CESER, but they often lacked the level of detail necessary to establish a strong and enduring cybersecurity program. This lack of detail was largely due to the limited project planning that could be conducted before contract award. Passing the plan through a pre-award acceptable phase allowed projects to begin work with the expectation that a more comprehensive and detailed cybersecurity plan would be developed. This is a perfect example of iterative planning. The projects provided as much detail as they could with the context they had in the moment, and then as they got more direction and guidance and advanced further in the development process, they were able to provide additional details to improve the plan and achieve an acceptable status.

Often as projects move into the build and implementation phase, the plan will be further detailed and integrated into the project's systems and processes. At this stage, real-world constraints often require reevaluating initial assumptions and adjusting security measures to ensure effective security falls within organizational standards and budgets.

Effective cybersecurity planning demands proactive refinement, collaboration, and adaptation throughout its lifecycle. Advanced threats and shifting organizational requirements often necessitate multiple revisions and consultations to ensure the plan remains relevant and effective over time. By embracing this approach, projects are given the flexibility to adapt, improve, and build out their plans as new information and real-world challenges emerge. The projects that have embraced this lifecycle approach are to be commended for their commitment to maturing their cybersecurity programs.

C. Submission Process

Most projects used CESER's January 2023 high-risk template [3] as is, but a few adapted it, which led to unproductive outcomes. Formatting adaptations were not problematic, but content adaptations often led to non-compliance, especially if questions were omitted. For example, one recipient chose to submit a corporate policy document without a cover letter or any other additional information instead of submitting their own plan. This submitted document was deemed non-compliant with the IIJA requirements because it failed to address the breadth of the questions specified in the high-risk template and because the recipient did not commit to follow the submitted policy document. The project was asked to use the provided template and encouraged to resubmit.

D. Acceptance Process

Upon the completion of each initial GRIP cybersecurity plan review, the plan is assigned to one of three status categories: *non-compliant*, *pre-award acceptable*, and *acceptable*, each with different follow-up actions/requirements for projects. Plans that were non-compliant with the cybersecurity requirements listed in IIJA Section 40126 were returned for revision. Pre-award acceptable plans are compliant with the CESER's IIJA requirements, but lack sufficient detail needed to ensure a strong cybersecurity program. This is typically because projects could not conduct enough project

planning prior to contract award, thus pre-award acceptable is a status that allows a project to start with an expectation that an updated cybersecurity plan will be developed within 60 days of contract award. Acceptable plans are compliant and rigorous enough to ensure that the project could execute a reasonable cybersecurity program as soon as the contract is awarded.

III. Summary of Plan Review Results

The cybersecurity plan review process encompassed submissions from 74 projects as part of the GRIP program. While most projects adhered to the mandatory template, a few deviated from the prescribed format. Of the initial plans submitted, 26 plans achieved an acceptable status, signaling their compliance and readiness for implementation. An additional 42 plans attained pre-award acceptable status, indicating they met minimum requirements but must provide further details once funding had been allocated. However, not all plans met the required standards; six were deemed non-compliant due to insufficient detail. Revisions by four GRIP-1 projects enabled their plans to subsequently achieve pre-award acceptable status. Plan updates from two GRIP-2 projects are expected in the future.

The distribution of acceptable and pre-award acceptable plans demonstrates diverse levels of cybersecurity planning maturity among the participants. The timely updates from 19 GRIP-1 participants highlights the commitment of these participants to constantly update their cybersecurity plans throughout the lifecycle of their projects. Future plan updates are expected from GRIP-2 participants once they have had additional time to review feedback.

IV. General Observations

A. Anticipated and Unanticipated Weaknesses in the Cybersecurity Plans

Most of the non-compliant and pre-award acceptable plans had observed weaknesses that can be grouped into two categories: anticipated weaknesses and unanticipated weaknesses. For the anticipated weaknesses, the review team provided initial training to the selectees. Since the plans were written before detailed project planning could begin, some lack of detail was expected. However, even with that expectation and the initial training on how to strengthen plans, several plans nonetheless had weak sections that needed to be addressed via updates to the plan.

The second set of observed weaknesses were unanticipated and likely resulted from a combination of inadequately phrased questions in CESER's high-risk template and an unexpected lack of cybersecurity maturity within some project teams. For these unanticipated weaknesses, the review team has developed or plans to develop additional training materials. The review team has also considered how possible changes to the questions in the high-risk template could elicit technically stronger responses.

B. Common Weaknesses in the Cybersecurity Plans

While some weaknesses were only found in a small minority of plans, some common weaknesses were found more broadly. These common weaknesses can be grouped into the following seven categories.

1) Vague management roles and responsibilities

One common weakness was the use of vague and overly broad language to describe management roles and responsibilities. In many cases, the descriptions failed to delineate actionable commitments or provide specific references to existing policies or frameworks. To be effective, cybersecurity plans must clearly articulate defined roles and responsibilities, ensuring actionable steps are grounded in established practices rather than generalized statements.

2) Reference to broad cybersecurity standards

Another trend was the frequent reference to broad cybersecurity standards without providing actionable details. While referencing established standards demonstrates awareness, the lack of specifics prevented the reviewers from assessing whether these references represented robust cybersecurity programs or general acknowledgments. Plans that lack detailed implementation strategies based on referenced standards present challenges in evaluating the adequacy of a cybersecurity framework. For example, rather than using a blanket statement like "we adhere to NIST 800.53" or even "this plan is based on NIST," neither of which provide actionable information, plans could point out the control strategies used within those domains that address the risk and technologies being discussed in the appropriate plan sections.

3) Repeated "cut-and-paste" answers

Several projects responded to many questions with uniform, repeated "cut-and-paste" answers. This would seem to indicate that the projects either chose not to spend enough time on developing their plans or the projects simply did not have the cybersecurity maturity to understand the difference between questions. By providing identical answers to distinct questions, projects often undermined the credibility of their plans, making it difficult for reviewers to assess whether the projects genuinely understood the complexities of cybersecurity planning.

4) Conflation of threat intelligence and vulnerability management

Plans often conflated threat intelligence and vulnerability management. Threat intelligence is outward looking (e.g., who is on the outside trying to get in), and vulnerability management has an inward focus (e.g., what is vulnerable inside my perimeter). These topics are distinct and should not be conflated in a high-risk cybersecurity plan. The review team developed new training materials to help projects understand the difference and in April and May 2025 presented this training during webinars on updating cybersecurity plans.

5) Weak supply-chain and third-party risk management

The high-risk template devotes an entire section to managing the supply-chain and third-party risk from a cybersecurity standpoint. With highly interdependent supply chains and increasing sophistication of supply chain attacks, these are increasingly important topics. However, many projects had weak supply-chain and third-party risk management sections. The review team plans to present future webinars and outreach activities to highlight the importance of

supply-chain and third-party risk management planning as part of a robust cybersecurity program.

6) Weak asset management

The strength of asset management responses varied widely, and many plans were weak in this domain. Operational technology (OT) asset inventories and configuration management were weaker than their Informational Technology (IT) counterparts. The identification and management of information assets (e.g., data) lagged both IT and OT asset management. Future training and assistance will be provided on this topic.

7) Lack of integration between project partners

Several projects involved multiple partners, and some of the plans for these projects lacked coherency and integration between the partners. Instead of reading as a single, unified plan, they instead read like multiple discrete plans with no overall direction or coordination.

C. Observed Strengths in Cybersecurity Plans

When viewed collectively, the GRIP cybersecurity plans demonstrated several recurring strengths. The following strengths *were not observed in all plans*, but they were observed frequently enough to represent the overall positive attributes of the GRIP cybersecurity plans as a group.

One prominent strength was the widespread use of appropriate industry standards. Many projects referenced well-established standards, demonstrating a foundational understanding of cybersecurity best practices. Notably, several projects enhanced their plans further by aligning their strategies with existing corporate policies based on these standards, showcasing maturity in their cybersecurity approaches. However, the quality of responses regarding standards revealed a bimodal distribution, with many projects either demonstrating a strong and comprehensive understanding or providing responses that were noticeably weaker, as noted in prior observations. This suggests that while some organizations have fully embraced standards-based frameworks, there is room for further education and consistency across all submissions.

Several organizations provided documentation of strong, existing cybersecurity programs. Such organizations were able to submit cybersecurity plans that demonstrate well-developed policies that reflect maturity across the organization. Acceptance and willing, active support of a cybersecurity program across all levels of an organization, from senior leadership to individuals, is required to provide the needed strategic vision, planning, execution, and implementation [5].

Many responses throughout the plans highlighted customized answers tailored to address specific questions, rather than relying on generic or standardized template language. This tailored approach added credibility to the plans, indicating that certain organizations took extra steps to thoughtfully evaluate their individual cybersecurity risks and provide meaningful solutions. Several submissions used strong frameworks that prioritized security measures based on the level of risk faced by the project or organization. While this strength was not uniformly observed in all plans, its presence in a significant proportion indicated an understanding of the dynamic nature of cybersecurity and emphasized the importance of prioritizing critical assets for enhanced protection. General cybersecurity training emerged as an existing requirement for most companies. This demonstrates that many organizations value ongoing cybersecurity education and training and have already integrated it into their operational procedures. The emphasis on providing training to key personnel reflects a foundational step toward building greater awareness and resilience in addressing cybersecurity challenges that target project staff.

These observed strengths provide valuable insights into the positive elements of many GRIP cybersecurity plans and serve as a foundation to guide further improvements and ensure a higher level of cybersecurity readiness across the sector.

V. Quantifiable Observations

A. Cybersecurity Plan Length

Cybersecurity plan length was loosely correlated with plan acceptance with shorter plans tending to have a lower acceptance rate. Since changes in formatting, such as font size, section breaks, etc., can result in different page counts for plans with similar content, the review team based their analysis of plan length on the word count instead of the page count. The CESER high-risk template has 5,817 words, with 1,713 words dedicated to the glossary and appendices. The initial cybersecurity plans ranged from 1,546 words to 49,820 words, with a median word count of 9,863 words and average word count of 10,709. The longest plan was an outlier at more than twice the length of the second longest plan, but removing it from the data did not have a large effect on the median or average word counts. Plans shorter than 5,817 words either used a custom template or omitted portions of the CESER-provided template such as the glossary and appendices.

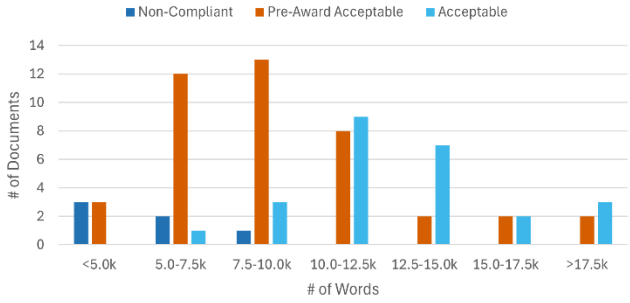

Figure 1 Word Count vs. Acceptance Status

As shown in Figure 1, non-compliant plans tended to be the shortest plans, while the acceptable plans ranged from moderately short to long. This is consistent with current guidance that document length is not a defining characteristic of a plan. A non-compliant plan may be shorter because the project had not yet completed detailed planning and therefore did not have much to document. By comparison, some project teams produced well-written plans that were double the length of other project plans, which clearly demonstrated greater cybersecurity maturity of the project team and their capability to easily document strong corporate policy.

B. *Cybersecurity Plan Complexity and Readability*

The Flesch-Kincaid Grade Level metric was used to evaluate the readability of the cybersecurity plans. The GRIP-1 and GRIP-2 plans had an average readability score of grade level 16, with most plans having a readability score between 14 and 17 as shown in Figure 2, indicative of advanced or post-graduate complexity. No significant correlation was observed between the readability of these plans and their acceptance status. Given the technical nature of cybersecurity plans, such high readability scores were anticipated. However, these elevated grade levels underscore the need for projects to include educated and well-trained personnel on their cybersecurity teams to effectively comprehend and implement the outlined strategies.

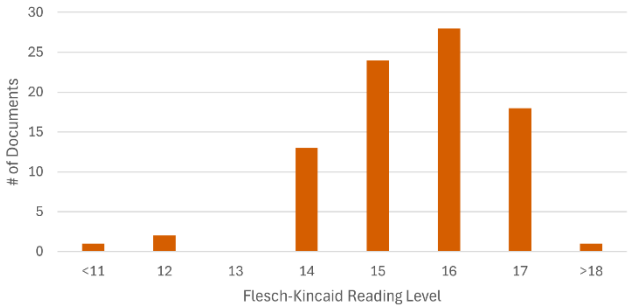

Figure 2 Flesch-Kincaid Reading Level Comparison

VI. Conclusion

Effective cybersecurity planning is an essential component of safeguarding critical systems and infrastructure, and the process of developing these plans requires careful consideration and collaboration. While cybersecurity plans are typically written for professionals in the field, meaning they require technical understanding to implement and maintain, the word count and length of a plan did not emerge as a significant factor influencing its acceptance status. This finding highlights that clarity, specificity, and relevance hold greater value than the breadth of content alone.

The use of mandatory templates in the plan development process revealed both advantages and disadvantages. Templates serve as a valuable tool, providing structured guidance to project staff, ensuring consistency across submissions. However, they also pose the risk of encouraging projects to adhere rigidly to the template rather than tailoring their plans to address unique cybersecurity risks specific to their operations.

There are key frameworks and standards that can be referenced, but if an 800-page standard alone is mentioned as being used without detailing how the associated control strategies will be implemented, it makes the reference un-useful to the review team as they cannot discern how it is meant to be incorporated.

Ultimately, the creation of a high-quality cybersecurity plan is a collaborative and iterative process. It involves aligning organizational efforts, engaging expertise from multiple stakeholders, aligning to well-established and accepted frameworks and standards, and continually refining strategies to ensure relevance and resilience against evolving threats. By prioritizing risk-based, actionable content and fostering effective teamwork, organizations can produce plans that not only meet compliance requirements but also strengthen overall cybersecurity posture. Often, a phased submission approach appears to work best, whereas the project will submit an initial draft during the design stage, get feedback, and then provide a more comprehensive plan that addresses any comments or concerns with additional details before the implementation, build-out, and operation of the system.

The review team at PNNL will continue incorporating these findings into training materials for GRIP project teams. GRIP awardees are expected to submit periodic updates to their cybersecurity plans over the lifetime of their projects. Emphasizing existing guidance and developing new training materials can help funding recipients improve their cybersecurity plans during these periodic updates by avoiding commonly observed weaknesses.

Acknowledgment

The authors would like to acknowledge the significant efforts of Pacific Northwest National Laboratory (PNNL) staff in the review and assessment of cybersecurity plans submitted across several U.S. Department of Energy (DOE) offices. These include the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the Office of Energy Efficiency and Renewable Energy (EERE), and the Grid Deployment Office (GDO). Their expertise and contributions have been invaluable in advancing the cybersecurity posture of these programs. The authors gratefully acknowledge the contributions of the following individuals for sharing their observations as part of the GRIP review team: A David McKinnon, Jesse Willett, Will Hutton, Richard Griswold, Travis Ashley, Jennifer Appiah-Kubi, Radha Kishan Motkuri, Paul Francik, Amy Pollom, Adom Cooper, Doug Castleman, Roger Kwon, Maria Psarakis, Sraddhanjoli Bhadra, Grace McNally, and Teresa Carlon.

References

[1] U.S. Department of Energy, “Cybersecurity Capability Maturity Model (C2M2),” U.S. Government. Accessed: Nov. 4, 2025. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[2] U.S. Department of Energy, “C2M2: About,” U.S. Government. Accessed: Nov. 4, 2025. [Online]. Available: https://c2m2.doe.gov/about.

[3] U.S. Department of Energy, “Cybersecurity Capability Maturity Model (C2M2) Version 2.1,” U.S. Government, Jun. 2022. Accessed: Nov. 4, 2025. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

[4] U.S. Department of Energy, “Cybersecurity Plan Template: High Risk,” U.S. Government, Jan. 2023. Accessed: Nov. 4, 2025. [Online]. Available: https://www.energy.gov/sites/default/files/2023-05/EXEC-2022-008113%20-%20Cybersecurity%20Plan%20Templates_High%20Risk.docx

[5] National Institute of Standards and Technology, “NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations,” U.S. Government, Dec. 2018. Accessed: Nov. 4, 2025. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/37/r2/final