A Case Study on Improving ICS Cyber Security Legislation

Ryan Gallagher, Melanie Gersten, Khalil Jackson, Deborah Liu, and James Massot –
NYU School of Law and NYU Tandon School of Engineering/NYU Center for Cyber Security
Edward Amoroso – *TAG Cyber and NYU Center for Cyber Security*
Kevin Senator and Toby Weir-Jones – *Bayshore Networks*

ABSTRACT

This paper introduces a framework to analyze the effectiveness of cyber security legislation. The framework is applied in this case to assess and propose improvements to a recently passed House of Representatives Bill focused on industrial control system security. The work described here is part of a larger research initiative sponsored by the New York University School of Law and the New York University Center for Cyber Security in the Tandon School of Engineering.

OVERVIEW

The Center for Cyber Security (CCS) at NYU sponsors research projects for graduate students seeking a master's degree in Cyber Security Risk and Strategy at NYU School of Law and the NYU Tandon School of Engineering. As part of this research, the authors and select partners have concluded an initial case study as part of their development of an assessment framework for cyber security legislation. This paper outlines that work and its recommendations.

Specifically, the research team reviewed a recent House of Representatives Bill that amended existing legislation to improve our nation's ability to deal with emerging cyber security risks to operational technology (OT) and the associated industrial control system (ICS) infrastructure. As most citizens know, the potential for malicious actors to tamper with ICS is both frightening and growing. The consequences of ICS cyber threats include:

- *Service Disruption* – Attacks to ICS infrastructure can result in severe disruption of essential national services including provision of power, water, and emergency services.
- *Safety Degradation* – In the worst cases, threats to ICS can result in loss of human life and other severe effects through degradation of safety systems.

- *Military Targeting* – ICS cyber attacks can have serious military consequences via targeted attacks at government services supporting the warfighter.

These potentially severe ICS consequences are obviously unacceptable, so our nation's leaders have come to recognize the need to act. The legislation under review was created to amend previously-passed cyber security legislation that did not specifically reference the security of ICS infrastructure. By increasing the Department of Homeland Security's (DHS) focus on ICS, the hope is that ICS security risk can be reduced.

To support this case study, we created an assessment framework and associated methodology to determine and improve the effectiveness of cyber-related legislation. Six factors make up the framework – *uniqueness, terminology, clarity, enforceability, attainability,* and *authority*. These factors, along with our methodology, were applied to the ICS legislation referenced above to demonstrate improvements that could be made to its effectiveness.

I. CYBER LEGISLATION FOR CASE STUDY

In selecting an initial piece of legislation for review, we wanted to select a work that was manageably small (our ongoing research is tackling more voluminous works). In addition, we wanted the selected legislation to be relevant to cyber security, which led us to focus on ICS, given its consequence. This led us to the US National Cybersecurity Protection Act of 2014 (NCPA), which amended the Homeland Security Act of 2002 [1].

Specifically, the NCPA authorized the National Cybersecurity and Communications Integration Center (NCCIC) within DHS. Enacted during the 113th Congress, this law established the NCCIC as the interface between the civilian federal government and non-federal entities for information sharing, risk analysis, and mitigation strategies related to cyber security. Since then, the NCCIC has been an effective component of cyber security operations at DHS.

The May 2018 House of Representatives (H.R.) Bill 5733, referenced as the DHS Industrial Control Systems Capabilities Enhancement Act of 2018 (DICSCEA), was written to amend ICS focus to the NCPA by requiring that DHS maintain capabilities in the NCCIC to support ICS threat identification [2]. The meaningful content of the Bill can be summarized as follows:

1. *Overall ICS Goal*: To maintain capabilities to identify and address threats and vulnerabilities to products and technologies for use in automated control of critical infrastructure.
2. *ICS Threat Mitigation* – DHS must lead, in coordination with sector specific agencies, all Federal Government efforts to identify and mitigate cyber security

threats to ICS, including supervisory control and data acquisition systems (SCADA).
3. *ICS Incident Response* – DHS must maintain cross-sector incident response capabilities to respond to ICS cyber security incidents.
4. *ICS Technical Assistance* – DHS must provide cyber security technical assistance to industry end-users, product manufacturers, and other ICS stakeholders to identify and mitigate vulnerabilities.
5. *ICS Vulnerability Coordination* – DHS must collect, coordinate, and provide vulnerability information to the ICS community by working closely with security researchers, industry end-users, product manufacturers, and other ICS stakeholders.

The precise text of the legislation is included as Appendix A. Throughout this case study, however, we reference the five content issues listed above, since other administrative issues in the Bill were deemed insignificant to this work. Appendix B includes a line-by-line assessment of the legislation based on our framework analysis and Appendix C includes a rewrite of the content portion of the Bill.

II. ASSESSMENT FRAMEWORK

Our case study involves comparing the summary goal and four points of DICSCEA against the six factors in a new assessment framework. The resulting artifacts are then used as the basis for a specific, detailed rewriting of each line of the Bill to bring it more in line with the intended goals of our assessment framework – namely, to make it more effective. The framework elements are as follows:

1. *Uniqueness* – Does the legislation break new legal ground in cyber security or does it replicate or restate existing law?
2. *Terminology* – Does the legislation use terms and language that are consistent with industry standards, or does it introduce new jargon?
3. *Clarity* – Does the legislation clearly relate the benefits to cyber security protection, or does it introduce vague statements of purpose?
4. *Enforceability* – Does the legislation include practical enforcement mechanisms, or does it impose unenforceable or unobservable conditions or requirements?
5. *Attainability* – Does the legislation facilitate outcomes and compel action, or does it threaten to have little impact? Does it establish practical implementation guidelines and timelines?
6. *Authority* – Does the legislation clearly identify authorities from a cyber perspective, or is it vague about responsibility for action? Are jurisdictional matters considered and addressed?

The methodology we propose involves three passes through a piece of legislation. First, the original legislation is subjected to a general, high-level assessment with respect to the six elements of the criteria framework. The Bill should be read broadly, and then an initial analysis should be made using the framework. We recommend pass/fail-type scoring for each element of the framework, but this can easily be mapped to a more granular scale.

Second, each line of the legislation should be subjected to a more specific, line-by-line assessment with respect to the six elements of the assessment framework. Each line should be read carefully, and then specific rewording, improved phraseology, and carefully chosen deletions should be made to the exact text of the legislation. The assessment framework should guide these decisions, in contrast to the more common ad hoc, subjective approach.

Finally, the rewritten legislation should be read broadly once more in the context of the changes made to each line. The goal is to ensure that issues identified in the first-pass broad assessment were addressed in the second-pass improvement. It is possible that missing elements, or high-level omissions might not be fixed by any specific line-by-line analysis and improvement of wording. The methodology is illustrated in Figure 1.

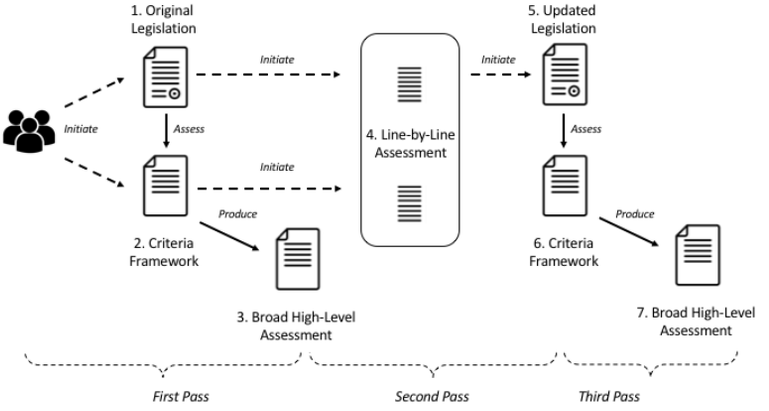

Figure 1. Three-Pass Methodology for Cyber Security Legislative Improvement

Our case study represents the first end-to-end exercising of this proposed methodology and framework. As our research progresses, we expect to develop refinements to the overall approach. For now, however, the six points listed above drive the effectiveness assessment covered here. We believe the effort has been successful, as our rewrite in Appendix C seems an improvement over the original Bill.

III. FIRST PASS ASSESSMENT OF DICSCEA

The initial, high-level assessment of the DICSCEA identified both strengths and weaknesses in the legislation, with respect to the criteria. The *uniqueness*, *terminology*, and *authority* categories were designated – at a high-level – to be covered well and basically *passed* the assessment. Rationale was that this Bill was not redundant with other Bills; no new industry terms were introduced; and the general authorities were clearly identified.

There were, however, some high-level weaknesses identified in the context of the framework. Many of the statements appeared too vague – such as "community" – and this brought some attention to the *clarity*, *enforceability*, and *attainability* of the legislation. References to "maintain(ing) capabilities" were also deemed vague, and introduced questions with respect to these three categories, resulting in *fail* assessments, respectively.

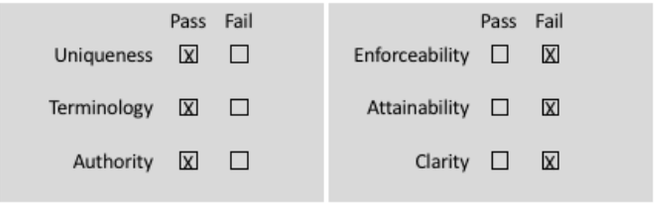

Figure 2. Results of First-Pass Assessment of Original DICSCEA

As shown in Figure 2, the result of the first pass of this assessment for DISCEA, based on a high-level, broad initial read of the legislation was *three passing grades* for uniqueness, terminology, and authority, and *three failing grades* for clarity, enforceability, and attainability. While no absolute conclusions can be drawn about the desirability of this combined score, clearly some enhancements could be made to improve the Bill.

IV. SECOND PASS ASSESSMENT OF DICSEA

The line-by-line assessment of the DICSCEA used the same criteria framework, but with a more focused view. That is, each content-rich line in the legislation was reviewed in the context of the six factors, and then a determination was made as to whether some wording improvement, change, or deletion might be made. This included some subjective judgment, but the criteria factors were helpful to maximize objectivity.

Each line of the DICSCEA included some aspect of its intent or construction that did not meet the goals of every factor of our framework. Stated more simply: We proposed changes to each line in the Bill. While the adjustments appear to be minor wording changes, they do provide substantive improvement to the overall Bill from an effectiveness standpoint. A summary which of the lines (i) through (v) included some sort of recommended change is listed below:

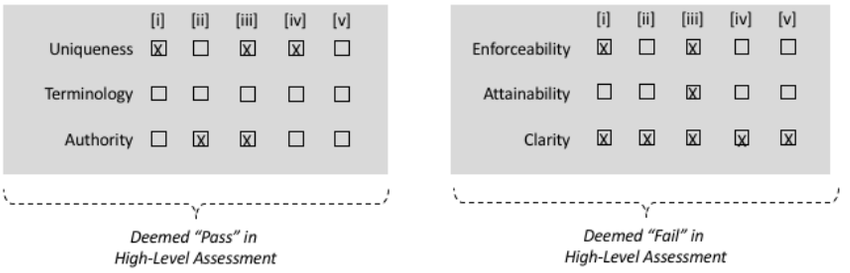

Figure 3. Summary of Line-by-Line Changes

Comparing the line-by-line assessment with the broad, high-level assessment suggests some degree of correlation. For example, the terminology factor, deemed a high-level pass, included no line changes (i.e. unchecked boxes in every column in Figure 3). Similarly, the clarity factor, deemed a high-level fail, included some recommended change for every line (i.e., checked boxes in every column). This suggests that for these two factors, both the high-level and low-level assessments came to the same conclusion.

For other factors, the correlation requires some interpretation. The uniqueness factor was deemed a pass in the high-level assessment, and the three line changes recommended by the low-level assessment are considered minor enhancements. Similarly, the two recommended line changes to the authority factor in the low-level assessment are considered minor, which is consistent with the overall pass grade for that factor.

For enforceability and attainability, both deemed a fail in the high-level assessment, while only minor changes are made in-the-small as part of the line-by-line analysis, both factors have a more holistic scope than the other factors. In general, all other factors generally contribute to the enforceability and attainability of the legislation. These two factors were thus improved by enhancements to other lines in the legislation.

V. THIRD-PASS RESULT AND CONCLUDING REMARKS

By making the changes to the original legislation, as proposed in the line-by-line analysis, the original legislation could be replaced with the updated text shown in Appendix C. The decision was made in this case study that no additional new content was required in the legislation to address remaining weaknesses in the final recommended product. The line-by-line updates produced an enhanced version of the Bill with an improved criteria score, as shown in Figure 4.

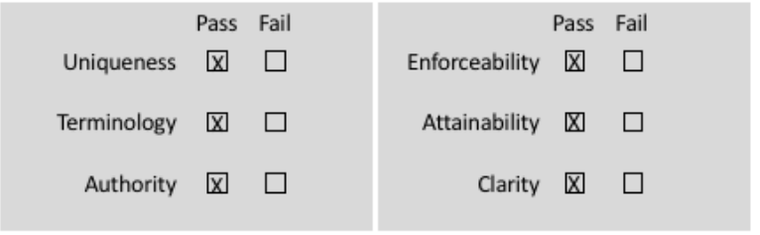

Figure 4. Results of Third-Pass Assessment of Enhanced DICSCEA

It is worth mentioning that our goal is to assist legislators in creating meaningful works that relate to cyber security. Extrapolating our assessment to other areas such as technology would be straightforward, but were outside the scope of this case study and research effort. The details of the politics, lobbying, and posturing required to pass any legislation were considered outside the scope of this work. Future research might focus in this area.

References

[1] Section 227 of the Homeland Security Act of 2002 (6 U.S.C.148). (https://www.congress.gov/Bill/113th-congress/senate-Bill/2519).

[2] DHS Industrial Control Systems Capabilities Enhancement Act of 2018, H.R. 5733, 115th Congress. (2018). (https://www.congress.gov/Bill/115th-congress/house-Bill/5733).

Appendix A: Original DHS Industrial Control Systems Capabilities Enhancement Act of 2018

This introductory section is necessary to amend Section 227 of the Homeland Security Act of 2002 (6 U.S.C.148).

"To amend the Homeland Security Act of 2002 to provide for the responsibility of the National Cybersecurity and Communications Integration Center to maintain capabilities to identify threats to industrial control systems, and for other purposes. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled; This Act may be cited as the DHS Industrial Control Systems Capabilities Enhancement Act of 2018. Sec. 2. Capabilities of National Cybersecurity and Communications Integration Center to Identify Threats to Industrial Control Systems. In General. Section 227 of the Homeland Security Act of 2002 (6 U.S.C.148) is amended – in subsection (e)(1) – (A) in subparagraph (G), by striking "and" after the semicolon; (B) in subparagraph (H), by inserting "and" after the semicolon; and (C) by adding at the end the following new subparagraph: "activities of the Center address the security of both information technology and operational technology, including industrial control systems;" by redesignating subsections (f) through (m) as subsections (g) through (n) respectively; and (3) by inserting after subsection (d) the following new subsection:"

Statements [i] through [v] constitute the substance of the Bill.

[i] *"Industrial Control Systems. – The Center shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Center shall –*

[ii] *(1) lead, in coordination with relevant sector specific agencies, Federal Government efforts to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;*

[iii] *(2) maintain cross-sector incident response capabilities to respond to industrial control system cybersecurity incidents;*

[iv] *(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, and other industrial control system stakeholders to identify and mitigate vulnerabilities;*

[v] *(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security*

researchers, industry end-users, product manufacturers, and other industrial control system stakeholders; and conduct such other efforts and assistance as the secretary determines appropriate."

The last section summarizes Congressional briefing obligations.

"Report to Congress. – Not later than 180 days after the date of the enactment of this Act, and every 6 months thereafter during subsequent 4-year period, the National Cybersecurity and Communications Integration Center shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the industrial control systems capabilities of the Center under subsection (f) of section 227 of the Homeland Security Act of 2002 (6 U.S.C 148), as added by subsection (a)."

Appendix B: Assessment Details

[i] *"Industrial Control Systems. – The Center shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Center shall –*

- *Uniqueness*. To make sure this Bill does not collide with any laws passed outside the US, or in state and local contexts, the word "**US national**" should be added to "critical infrastructure."
- *Terminology*. No changes. The terminology of the Bill is excellent and does not introduce any new concepts or terms that could cause confusion.
- *Clarity*. To make referenced capabilities clearer, the phrase "**reasonable, state-of-the-practice**" should be appended to "capabilities." Also, to make the referenced products and technologies clearer, the word "**common**" should be appended to "products and technologies."
- *Enforceability*. To make the overall goal more targeted and enforceable, the phrase "**related to industrial control systems and operational technology-based infrastructure**" should be appended to the entire sentence.
- *Attainability*. No changes. This aspect of the Bill looks reasonable and attainable in practice across the ICS community.
- *Authority*. No changes. No issues are raised in this section of the Bill that would cause confusion about authority either within DHS or across Government.

[ii] *(1) lead, in coordination with relevant sector specific agencies, Federal Government efforts to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;*

- *Uniqueness*. No changes. This second content statement does not conflict with other legislative works.
- *Terminology*. No changes. The terminology in this statement is acceptable and standard.
- *Clarity*. To make referenced Federal Government efforts clearer, the phrase "**support prevention, detection, and response-related activities**" should be used. Also, to make the referenced industrial control systems clearer, the phrase "**critical US national**" should be added.
- *Enforceability*. No changes. Enforcement issues are not raised in this statement.
- *Attainability*. No changes. Attainment issues are not raised in this statement.
- *Authority*. To ensure a more accurate description of Federal organizations in scope, the phrase "**departments and**" should be added.

[iii] *(2) maintain cross-sector incident response capabilities to respond to industrial control system cybersecurity incidents;*

- *Uniqueness*. To make sure this Bill does not collide with other laws outside the country and to ensure that it focuses on the correct infrastructure, the phrase "**address critical US national**" should be added.
- *Terminology*. No changes. The terminology of the Bill is excellent and does not introduce any new concepts or terms that could cause confusion.
- *Clarity*. To make referenced capabilities clearer, the phrase "**develop and manage state-of-the-practice**" should replace "maintain."
- *Enforceability*. To make the overall goal more targeted and enforceable, the phrase "**with focus on supporting actionable decisions across the Federal Government and any US national industrial control system entities affected by the incident***"* should be added.
- *Attainability*. No changes. This aspect of the Bill looks reasonable and attainable in practice across the ICS community.
- *Authority*. No changes. No issues are raised in this section of the Bill that would cause confusion about authority either within DHS or across Government.

[iv] *(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, and other industrial control system stakeholders to identify and mitigate vulnerabilities;*

- *Uniqueness*. To make sure this Bill does not collide with other laws outside the country and to ensure that it focuses on the correct infrastructure, the phrase "**that can affect US national critical infrastructure**" should be added.
- *Terminology*. No changes. The terminology of the Bill is excellent and does not introduce any new concepts or terms that could cause confusion.
- *Clarity*. To make referenced capabilities clearer, several changes are recommended: The phrase "**expertise, intelligence, and consultation**" should replace "assistance;" and the phrase "**prevent, detect, recover, or respond**" should replace "identify and mitigate."
- *Enforceability*. No changes. This is fine from an enforcement perspective.
- *Attainability*. To make this more attainable, the phrase "**reasonable, state-of-the-practice**" should be added before "cybersecurity technical."
- *Authority*. While this is not directly related to authority, the phrase "**security researchers**" should be appended to the list of targeted stakeholders.

[v] *(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, and other industrial control*

system stakeholders relating to domestic critical infrastructure; and conduct such other efforts and assistance as the secretary determines appropriate."

- *Uniqueness*. No changes.
- *Terminology*. No changes.
- *Clarity*. To make referenced vulnerability-related actions clearer, the phrase "**collect, protect, and discretely provide relevant**" should replace "collect, coordinate, and provide."
- *Enforceability*. No changes.
- *Attainability*. No changes.
- *Authority*. No changes.

Appendix C: Rewrite of DHS Industrial Control Systems Capabilities Enhancement Act of 2018

[i] *"Industrial Control Systems. – The Center shall maintain* **reasonable, state-of-the-practice** *capabilities to identify and address threats and vulnerabilities to* **common** *products and technologies intended for use in the automated control of critical* **US national** ***i****nfrastructure processes* **related to industrial control system and operational technology-based infrastructure**. *In carrying out this subsection, the Center shall –*

[ii] *(1) lead, in coordination with relevant sector specific* **departments and** *agencies, Federal Government efforts to* **support prevention, detection, and response-related activities for** *cybersecurity threats to* **critical US national** *industrial control systems, including supervisory control and data acquisition systems;*

[iii] *(2)* **develop and manage state-of-the-practice** *cross-sector incident response capabilities to* **address critical US national** *industrial control system cybersecurity incidents* **with focus on supporting actionable decisions across the Federal Government and any US national industrial control system entities affected by the incident***;*

[iv] *(3) provide* **reasonable, state-of-the-practice** *cybersecurity technical* **expertise, intelligence, and consultation** *to* **security researchers,** *industry end-users, product manufacturers, and other industrial control system stakeholders to* **prevent, detect, recover, or respond to** *vulnerabilities* **that can affect US national critical infrastructure***;*

[v] *(4)* **collect, protect, and discretely provide relevant** *vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, and other industrial control system stakeholders; and conduct such other efforts and assistance as the secretary determines appropriate."*