SHAPING STRONG SECURITY NORMS

"Duty Of Care" for Security in Nuclear Facilities Through Organizational Governance

STIMSON

OCTOBER 2018

Cover Photo: H. Mark Weidman Photography/ Alamy Stock Photo

STIMSON
1211 Connecticut Ave. NW, 8th Floor
Washington, D.C. 20036
Tel: 202.223.5956 | Fax 202.238.9604
www.stimson.org

TABLE OF CONTENTS

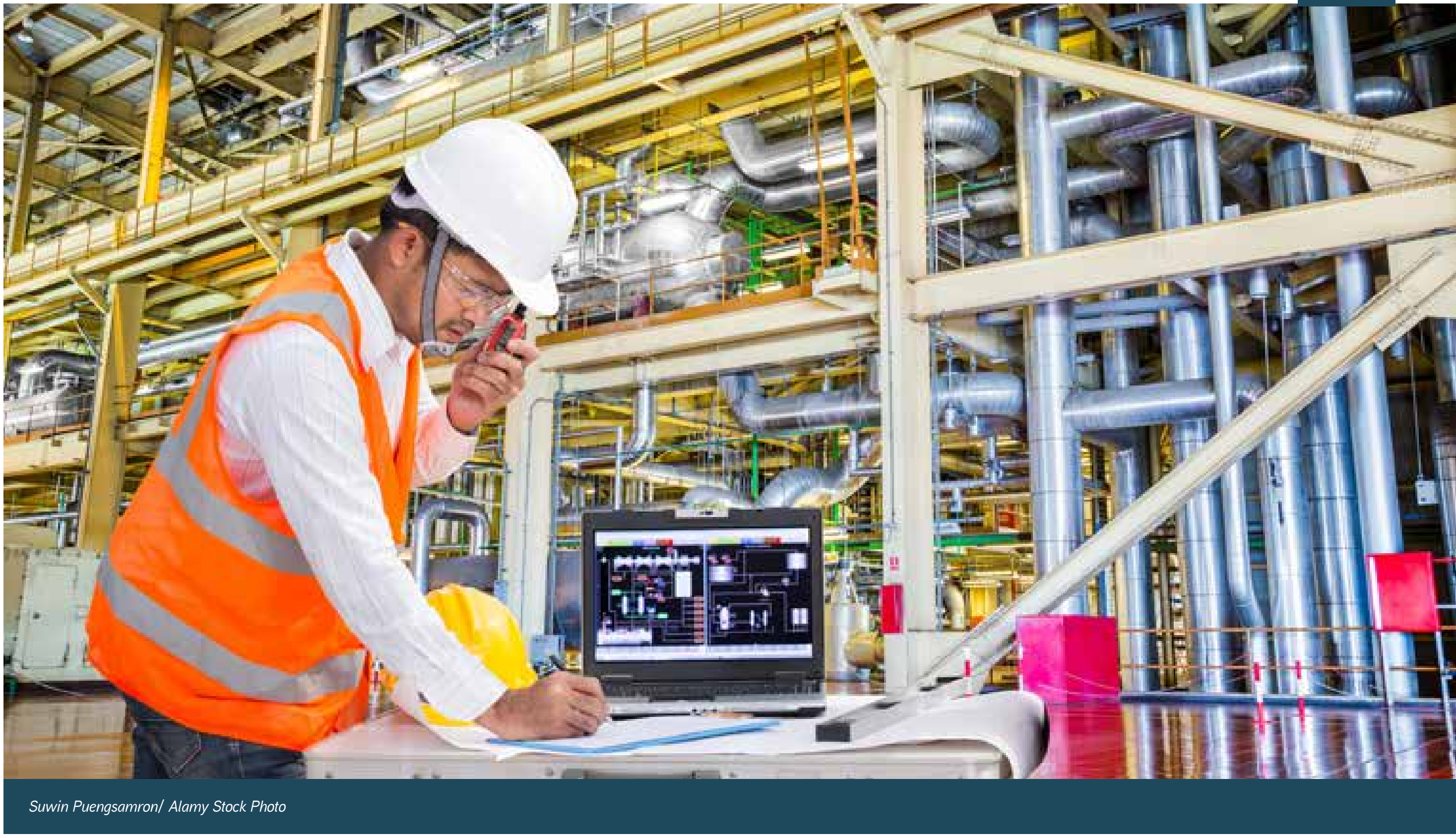
SHAPING STRONG SECURITY NORMS

"Duty Of Care" for Security in Nuclear Facilities Through Organizational Governance

The future of nuclear energy is at a crossroads—experts, governments, and industry are locked in debate on how to best seize opportunities and to steer clear of challenges ahead.

Today, there are over 400 nuclear power reactors operating around the world, generating 10.5% of the world's electricity production.[1] While more than half of these reactors are set to retire in the coming decades, compounded by several abrupt premature closures prompted by increasing market competition, nuclear power continues to play a pivotal role in diversifying and meeting energy demands worldwide.[2] Fifty-five reactors are currently under construction, and given concerns about rising temperatures and its inevitable deleterious impact on the world's climate, many countries are showing renewed interest in nuclear as a technologically viable option for carbon-free energy.[3] But amidst this opportunity to encourage favorability towards nuclear energy, public reservations about nuclear safety and security persist. While safety continues to garner the most attention both in the form of public critique and industry response, security is a rapidly rising contender.

Cyberattacks are changing the nature of security and the ways we think about it. While large-scale terrorist acts are still of paramount concern, far easier access to advanced technology—both in the form of equipment and know-how—has opened the possibility for stealthier, prolonged campaigns allowing malicious actors to discreetly and effectively exploit security vulnerabilities. It comes as no surprise that cybersecurity has garnered rapt attention across all business sectors. In 2017, about 160,000 attacks were executed worldwide ranging from ransomware attacks to email hacks (the number may be higher since not all incidents are reported).[4] And in 2018, the global average cost of a data breach is estimated to be a total of $3.86 million.[5] Critical infrastructures have also been disrupted; in the past year alone, the sector has been hit with infectious ransomware with indiscriminate global reach, as well as multi-layered attacks with clear strategic targets.[6]



Suwin Puengsamron/ Alamy Stock Photo

Not all attacks are executed from the outside; unwitting insider threats—individuals within an organization that inadvertently aid an attack without being aware of it—are on the rise, primarily in the finance and communication sectors.[7] Critical infrastructures can also fall victim to unwitting insider threat; investigators found that the cyberattack on Ukraine's power grid in 2015, which left more than 200,00 customers without power, was initially carried out via a spear-phishing scheme, nine months prior to the actual business disruption.[8]

The alarming rise of cyber incidents every year is eroding public confidence in the ways companies and organizations conduct business. In 2016, Pew Research found that as more Americans experience data theft, they lose faith in public and private institutions' ability to protect digital data. About 28% of Americans noted that they are *not at all* confident that the federal government can protect data, compared to only 12% who are very confident.[9] Naturally, business executives are beginning to feel the heat—in a cross-sector 2017 senior executive and risk professional survey, reputational fallout was cited as the second greatest potential impact resulting from a cyber event (the first being business interruption).[10] Reputational harm can manifest not only in loss of customers, but also potential collaborations or investors due to a tainted brand.

Thus, these real-world cases behoove all businesses, including those in the nuclear sector, to reflect and reconsider how they prioritize and handle security to properly defend against attackers. In fact, several nuclear operators acknowledged that in order to excel in security-related matters, the "approach goes beyond simply meeting regulatory requirements."[11] But the learning curve is steep. Determining proper security, including adequate cyber protection, and ensuring reliable implementation goes beyond the traditional guns, guards, and gates formula. Security, like safety, must also be embedded within the organizational culture of a nuclear facility; a strong belief that a credible threat exists at every level of the workforce is a key element in making informed security decisions at the top of the management chain, as well as effective execution at the operational level.[12]

But there are some significant barriers that impede belief in a credible threat, likely caused by knowledge gaps along managerial lines about what a facility's threat profile actually looks like. More often than not, this is a case of incomplete information and miscommunication, and not of sheer apathy or negligence. The lack of senior-level situational awareness about the threat and security vulnerabilities could make it difficult for decision-makers to conceptualize risk and make the appropriate call to improve security measures.[13] And with the growing sophistication of cyberattack vectors to maneuver through operational processes or exploit human error, conversations about threats and risks must now be a continuous organizational exercise such that security responses are both proactive and adaptive. Many cyber-nuclear security specialists are encouraging facility operators to think about cyberattacks as inevitabilities, rather than possibilities—it is no longer a question of *if*, but *when*.[14] This mindset cannot be bought or externally imposed; it must be intrinsically valued, promoted, and upheld across the workforce.

There is no one-size-fits all approach to security culture, but stakeholders within the nuclear community are beginning to recognize the value in determining what "security culture" means and looks like within their respective roles. At the international level, security culture is designated a *Fundamental Principle* for nuclear security under the recently amended Convention on Physical Protection for Nuclear Material (CPPNM). Thus, states party to the Convention must commit to implementing security culture in *all organizations* handling civilian nuclear material.[15] Security culture self-assessments are highly recommended by the IAEA as a way for operators to gauge how the *human* element in a facility—current perceptions, attitudes, and beliefs—compose the optimal (or inadequate) behavior towards security threats and vulnerabilities at a given moment in time.[16] But as it stands, security culture self-assessments are not required by most nuclear regulators, and are treated as a best practice. The demands of a constantly shifting security landscape, as well as growing public interest in organizational accountability and transparency around security issues, can lead to new opportunities for nuclear stakeholders to underscore their strong organizational commitment to security culture.

Stimson, in consultation with nuclear security specialists, regulators, insurers, lawyers, and facility operators, propose a model that encourages nuclear facilities to demonstrate their "duty of care"—the ways in which operators, particularly at the executive and managerial levels, take ***reasonable care*** or exercise ***reasonable skill*** to address foreseeable threats and correct security vulnerabilities—in a way that would be defensible to a judge or jury.[17] The proposed model, the ***Organizational Governance Template for Nuclear Security***, aims to illustrate that providing a clear narrative on how senior leadership prioritize, cultivate, and maintain strong security culture in their workforce can be a competitive advantage not only to industry, but the wider nuclear security enterprise.

THE STIMSON APPROACH

Encouraging Common Ground Among Disparate Perspectives On Nuclear Security

While experts, governments, and industry representatives all agree that nuclear security is a critical global issue, each of these stakeholders still view the problem through different prisms, engendering debate on how much attention it should receive. For instance, some countries, such as the United States, urge stronger international commitments for nuclear security due to heightened concerns about non-state actors stealing and trafficking nuclear or radiological materials, or worse using them to commit a terrorist act. But some states do not see nuclear security as an immediate concern and are likely to prioritize and allocate resources towards non-nuclear challenges that they perceive would pose greater local or regional consequences. While political will exists, resources may not be readily available.

Within industry, nuclear power operators are required to implement a risk-informed approach in allocating its resources for nuclear security measures. Recommendations to voluntarily adopt additional security measures beyond what is required often generate a spirited debate on what this looks like in practice. Operators, for instance, caution that “strong” security should not necessarily mean “more” security, but perhaps a rightsizing process to ensure that existing measures are still adequate as threats change and new vulnerabilities are found overtime. Imposing additional security requirements on industry without taking into consideration how it would affect other aspects of operations could impede rather than benefit business. But some experts worry that the standard procedure is still driven by checklists, which disincentivizes working-level personnel from remaining alert and responsible during their

H. Mark Weidman Photography/ Alamy Stock Photo

The Stimson Center hosted a Nuclear Security Roundtable: Demonstrating Strong Governance and Due Care, London, October 2017.

duties. As seen in high-profile cyber incidents in nuclear power plants, including the 2003 Davis-Besse incident in the United States, as well as the 2016 incident in Germany's Gundremmingen nuclear power plant, security lapses stemmed from violating basic cybersecurity protocols such as prohibiting the use of portable devices in restricted areas, or updating patches regularly.[18]

These varying views are further divided by the fact that there are limitations to discussing security among different stakeholders, thereby restricting information sharing and ultimately preventing a holistic view of the issue. Despite these differences, the consequences of an undesired event bind them together—a security incident in one facility, if found egregiously negligent in their security procedures, can have a massive spillover effect on the rest of the nuclear sector.

As part of its multi-year research effort, the Stimson Center—Nuclear Security Program has posed the following question to different actors within the nuclear community:

What cost-effective ***tools*** can we build to encourage proactive security culture around the world, especially as the ***security landscape shifts*** in ways that could impact how we protect nuclear facilities and materials in the future?

Through this question, Stimson aims to provide common ground among seemingly disparate groups and encourage a productive conversation on (1) how to change prevailing assumptions that nuclear security is a resource-intensive endeavor; and (2) how to incentivize proactive thinking around nuclear security, even when regulatory requirements are being fulfilled.

After three years of research consisting of cross-sector interviews and roundtable events, various stakeholders have shown support in promoting the idea of "duty of care" for nuclear security and Stimson's proposed *Organizational Governance Template for Nuclear Security,* as these concepts present a workable solution that acknowledges different, and at times conflicting, perspectives.

THE IMPORTANCE OF "DUTY OF CARE" FOR NUCLEAR SECURITY

A Legal Lens

> Negligence is the omission to do something which a reasonable man, guided upon those considerations which ordinarily regulate the conduct of human affairs, would do, or doing something which a reasonable man would not do.
>
> BLYTH V BIRMINGHAM WATERWORKS (1856) 11 EX 781 PER ALDERSON B AT 784[19]

Liability for the operation of nuclear facilities is complex, and in some cases, not well understood. While an international liability regime already exists to covers incidents that release radiation, other events such as a disruption to the electrical power supply from a nuclear power plant are not included in this coverage.[20] Energy security and the importance of protecting energy infrastructure from terrorists cannot be overstated. To better understand the range of liabilities owing to non-radiological incidents, the Stimson Center conducted workshops where participants examined hypothetical scenarios in which the adversary's goal was to disrupt routine reactor operations to cause a blackout. Participants agreed that a physical, cyber, or hybrid attack to a nuclear facility that takes out the supporting infrastructure would be difficult but not impossible to affect.[21] As mentioned above, recent real-life incidents demonstrate that this is now a feasible scenario: The U.S. Department of Homeland Security and the Federal Bureau of Investigation recently reported that Russian hackers were able to infiltrate nuclear power plants remotely and with relative ease. The report analyzing the incident noted that the attackers took great care to cover their tracks, making it difficult to determine the extent of the damage or intent to sabotage.[22] More recently, a senior official at the U.S. Department of Energy admitted during a congressional testimony that American utilities are not adequately prepared to withstand increasingly sophisticated cybersecurity attacks.[23]

Even a temporary power outage at a nuclear power plant could lead to severe consequences and costly litigation. Third party liability claims for personal injury, business interruption, reputational harm in addition to potential regulatory fines and penalties could be substantive. Given the complexities associated with liability for such

PERSPECTIVES FROM THE BENCH

T.J HOOPER

In the precedent-setting **T.J. HOOPER MARITIME CASE** of 1932, a tugboat without a functioning radio receiver was caught in a storm, and all its cargo was lost at sea. Judge Learned Hand evaluated whether the operator's decision *not* to install a radio was a reasonable operational decision. The tugboat operator argued that because other tugboats in the area were not using radios, its conduct met the prevailing or common practice in the industry and was therefore reasonable. While this at first blush appears to pass the test of reasonableness, Judge Hand determined that "common practice" is not the same as "reasonable practice" because there was readily available technology (radio broadcasts) which would have alerted them to the hazard. The cost of the radio would have been far less than the loss of the cargo. It is important to remember that what is "reasonably practicable" changes as technology advances. The swiftness of technological change and requires a continuous re-examination of those cost-benefit decisions.[24]

1993 TRADE CENTER

The **WORLD TRADE CENTER BOMBING CASE** in 1993 illustrated how failure to act on information from a security audit can form the basis for corporate liability. An audit or assessment puts the owner/operator on notice of potentially dangerous conditions which could give rise to civil or criminal liability. In this case, the Port Authority was warned of the risk of a car bomb in external security audits prior to the bombing in February of 1993. Citing the loss of parking revenues, the Port Authority rejected an audit recommendation to close public parking areas to prevent a bombing and opted for less expensive security measures. The negligent failure to act on this recommendation allowed the terrorists to enter the garage unimpeded and park a van next to vital utility and communications systems. Civil lawsuits filed after the bombing alleged breach of the landlord's duty to keep its premises reasonably safe when it failed to implement adequate security measures.[25]

LOCKERBIE BOMBING

The **LOCKERBIE BOMBING CASE** also demonstrates failure to implement adequate security measures. Pan Am was found guilty of "willful misconduct", due to lax security when in December of 1988, Pan Am flight 103 exploded over Lockerbie, Scotland. The bomb was hidden in a suitcase which went from Malta to Frankfurt, Germany. The unaccompanied bag was transferred to a Pan Am flight to London and then to Flight 103. The plane exploded over Scotland thirty-eight minutes after takeoff from London, killing all 259 passengers aboard and 11 on the ground. The luggage was not subjected to a Federal Aviation Administration Directive, which would have required a physical inspection and identified the bag as unaccompanied. Pan Am made a cost-benefit decision to forgo adopting the measure which would have matched the luggage, and instead opted for an administrative screening in which bags were simply x-rayed and put on board, rather than matched against specific tickets. This case illustrates how non-conformance with an international standard can be used as a metric for "reasonable conduct" against which negligence can be measured.[26]

an incident at a nuclear facility, it is important that corporate executives understand the implications for their responsibility, accountability, and liability should a nuclear security event occur. In the context of a cyber-physical attack on a nuclear facility, the most likely form in which liability would be tested is in a tort suit alleging that the entity (i.e., the nuclear operator) acted negligently by failing to exercise reasonable care or due care in preventing an attack. Since there is no precedent to draw from in the nuclear sector, cases from other sectors such as civil aviation are rapidly forming a body of law around negligent security and the failure to exercise reasonable care in preventing a security incident.

H. Mark Weidman Photography/ Alamy Stock Photo

The concept of reasonableness is at the center of legal jurisprudence in negligence tort law. In addition to complying with regulations, industry is increasingly being called on to demonstrate that their actions were reasonable under the circumstances. Historically, industry norms and best practices have been looked to in demonstrating reasonableness. However, the expectations of a given community change over time and in an era of innovation and rapidly evolving technology, companies may not be able to get by with just meeting the preventative measures of their peers. For instance, the lesson from Judge Learned Hand (see inset) for practitioners in cyberspace is that the prevailing practice is not always sufficient if there is a readily available technology that could have prevented an incident. Thus, the proposed governance template may serve as important resource showing that a company adopted "basic legal hygiene" given that they have taken care to *document* and *demonstrate* how and why risk management decisions were made. As the concept or reasonableness can be exceedingly vague, the governance template could help the trier of fact comprehensively and fairly evaluate whether an operator's security decisions were reasonable under the circumstances and form a first line of defense.

LIGHTS OUT: TESTING REASONABLE SECURITY THROUGH CYBERATTACK SCENARIOS

Across all business sectors, traditional security approaches are struggling to keep pace with a dynamic cyber threat environment. Attacks are no longer one-off events, but multi-stage campaigns that initially lay dormant until the time is ripe to execute the main thrust of the offensive, may that be in the form of physical sabotage, data exfiltration, or digital extortion. Attackers are also prone to cast a wide net and do not typically target just a single entity but are likely to lay out plans that have systemic impact.[27]

At the heart of the issue is limited awareness within organizations on how the human factor—a seemingly inconsequential personnel inaction or mishap, for example—can create the perfect opportunity for cyber adversaries to bypass existing security measures. So, what can organizations do so as not to be blind-sided by unknowns that derail what were thought to be sound security protocols?

A good first step is to test long-standing assumptions on what is considered "secure." During a Stimson-hosted nuclear security roundtable, cybersecurity specialists and facility operators debated the notion of nuclear facilities being "air-gapped," a security process that separates a *high* computer network (i.e., operations network and industrial control system of a nuclear facility) from all other *low* or less-sensitive networks that use the Internet for business purposes.[28] A cybersecurity expert explained that a threat actor can now easily reconfigure hardware commonly found in facilities—routers and data diodes, for instance—that control and separate traffic between the *high* operations and *low* business networks. By manipulating the flow of traffic through a data diode, an attacker could maneuver around existing firewalls to access the *high* side of the network, ultimately leaving it vulnerable to further sabotage. Several human errors can contribute to this scenario, including staff falling for a phishing scheme that would allow attackers initial entry into the system, as well as IT personnel failing to secure their routers by deactivating Auto or Smart Install features that are typically included in off-the-shelf routers for easy installment (in this case, it would be best practice to disable this feature immediately after install).

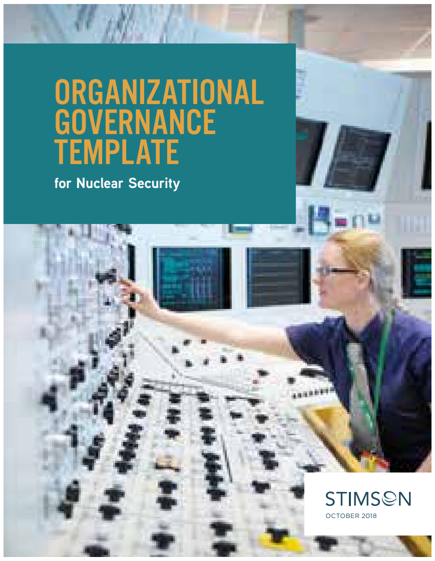
By discussing this situation, two assumptions are challenged: (1) Infiltrating secure, operational networks require external, physical movement and intrusion via flash drives or similar means. Recent cases have shown that it is now possible to jump from business to operation networks easily.[29] Understandably, organizations cannot protect from every imaginable type of attack, but it is best practice to regularly revisit security criteria and contingency plans to ensure that they still reasonably address the threat as adversarial capabilities evolve. (2) Just because hardware or software are working as expected does not make them necessarily secure. In the scenario, the router was not defective, but the Smart Install feature became an unassuming entry point for a cyber adversary because IT personnel failed to remove disable it after installation. Knowing what to omit is just as important as knowing what to implement, but few organizations actively train staff for this type of awareness and competence.

Cybersecurity experts and facility operators also agreed that these operational errors are almost always rooted in a lack of managerial support and investment towards security training or standards. Security awareness cannot be achieved through a grass-roots approach; organizations that have a strong security plan do not solely rely on operational staff to implement and maintain this code of conduct on their own. Rather, it must be directed and funded by the people at the top of the chain.

A PROPOSED GOVERNANCE TEMPLATE

Articulating Duty of Care for Nuclear Security

In 2016, the Stimson Center, in partnership with the World Institute for Nuclear Security (WINS), began work on the *Organizational Governance Template for Nuclear Security*, a resource that invites nuclear operators, specifically those with leadership roles within the site, to describe their process of building and sustaining a robust security culture within their workforce. Originally a 10-question survey, the governance template has since expanded to include topics and themes based on existing guidance documents from the International Atomic Energy Agency. It also incorporates insights from the World Association of Nuclear Operators (WANO) and the U.S.-based Institute of Nuclear Power Operators (INPO) industry guidance for safety as these leadership recommendations can also help develop strong nuclear security practices. The governance template provides a way for senior leadership within a given facility to take a snapshot of their organizational decision-making process on security-related matters, and how this ultimately impacts the beliefs and attitudes of those at the operational-level tasked as the responsible stewards of nuclear material and technologies. ***Overall, the goal of the governance template is to promote transparency by enabling individuals outside an organization to understand how the organization/company demonstrates its "duty of care," i.e., not only by adhering to minimum regulatory requirements but also by fostering a work environment that promotes continuous improvement, adapts to evolving risks and embeds nuclear security as a core value.***[30]



ORGANIZATIONAL GOVERNANCE TEMPLATE

for Nuclear Security

STIMSON

OCTOBER 2018

VALUE PROPOSITION OF THE GOVERNANCE TEMPLATE

EXTERNAL COMMUNICATION TOOL

Narratives are an important part of effective communication; stories help people better understand the human impact of data, especially in illustrating a commitment to security by the community of people that work in a nuclear power facility. The governance template provides an outlet for leadership to transform data-driven security processes and policies into a narrative that is approachable and meaningful to the public, as a way to build confidence and trust.

INTERNAL PERFORMANCE ASSESSMENT TOOL

The governance template serves as an internal assessment and gap analysis tool for nuclear facilities, particularly in determining whether senior leadership has consistent understanding of, and commitment to security culture by way of policy and in practice. In addition, highlighting areas where an organization is doing well offers opportunity to reward good behaviors that might otherwise not be recognized. Overall, this helps to build common language and intent across a diverse workforce and offers snapshots of nuclear security improvement overtime.

LEGAL NARRATIVE TO DEMONSTRATE REASONABLE PRECAUTION

In the event of a third-party liability lawsuit arising out of alleged failures by the company to detect and address risks, the governance template provides a prepared set of written enterprise risk mitigation protocols illustrating that the organization regularly assesses risks and insures that its personnel are trained on key techniques to identify and address risks.

The governance template includes questions arranged under four key themes found in existing nuclear security documentation: Leadership and Oversight, Nuclear Risk Assessment, Shared Understanding of Nuclear Security, Evaluation and Continuous Learning. Taking into consideration preliminary input from industry and regulatory reviewers, the updated draft is formatted such that questions are directed to specific leadership positions in a facility, including Chief Operating Officers, Chief Security Officers, Chief Nuclear Officers, and Site Management. Arranging questions that speak to these different managerial roles levelized the governance template such that questions are being answered by the appropriate and most qualified plant personnel.

Most operators already have some form of assessment that gathers similar information about security culture based on rating scale surveys sent to site personnel. The governance template aims to compliment this data by offering open-ended questions that allow for narrative responses from key executive actors that help make decisions on what security measures to prioritize, as well as personnel actions that should be rewarded or disciplined due to their impact on the security of the facility. Such a narrative can provide an in-depth understanding of how humans perceive, interpret or respond to security threats in real-time, and under real circumstances. These insights are critical to strategic planning, as they reveal the results of previous strategies, and assist in forging a path forward with these results in consideration. Thus, the governance template can serve two roles: as an internal assessment and tracking mechanism used to develop new strategic planning, as well as a means of *storytelling* that can help an organization communicate its commitment to security to various stakeholders, including its board members, shareholders, or even the public.

CHAMPIONING REPUTATION AND TRANSPARENCY

TERRY YOUNG

> If you ask me the top 10 things I worry about, nuclear power isn't one of them. That is, until the plant in my backyard makes news. You see, we have a ***deal***. It's not written anywhere but it goes like this. I'll let you run that nuclear plant—that's right I'll let you—as long as you don't make me worry about it. I assume you keenly understand our deal—that you operate at the pleasure of the public. I assume you have a strong federal regulator that keeps track of your every move so you don't pump nuclear waste into the river…or worse. And I assume you do everything you can to live up to your end of the ***bargain***. I have to assume all these things—otherwise I couldn't bear to live next to your plant.
>
> TERRY YOUNG, WOLF CREEK NUCLEAR OPERATING CORPORATION

Public trust falters when companies and organizations do not live up to their obligations, including assurances that their conduct will not harm the public in any way. Hence, retaining public trust requires organizations and companies to pull back the curtain to prove that they are upholding their end of "the deal."

How can they communicate that the deal is being honored? In today's digital environment, most organizations are prone to inundating the public with data highlighting the absence of safety and security incidents. But human beings are not driven by data; public outrage in response to a company's failure to secure private information or public safety is an emotional response. While accurate, data-driven messaging does not deliver an emotional connection. Thus, storytelling is essential in communicating an organization's value of nuclear security to the public. The method of delivery matters just as much as the information itself.

As one industry representative put it, stakeholders in the civilian nuclear community are "hostages of each other" when it comes to potential safety and security incidents. Everyone sinks or floats together based on public confidence. If one facility is viewed as dangerous, the public is likely to view the entire industry as being unsafe. Nuclear power providers must be honest about the risks involved and be willing to illustrate their commitment to protecting employees and the public.

THE GOVERNANCE TEMPLATE IN PRACTICE

The governance template is designed to fit into existing processes within nuclear facilities so as not to create redundant procedures for senior leadership to navigate through. Hence, effective implementation will require a conversation and collaboration among senior leadership within an organization such that the governance template is seamlessly embedded into current processes, and to ensure that it is helping address specific needs. As part of determining the best path for implementation, Stimson experts will conduct a consultation process with relevant senior management to review the governance template and discuss the best way to integrate it into existing organizational procedures, standards or assessments.

In operationalizing the governance template, the following issues will be covered:

1. GOVERNANCE TEMPLATE COORDINATION AND OWNERSHIP

In the process of integrating the governance template into a company or organization, it will be important to identify a *coordinator*, i.e. the individual or group that will act as a focal point for implementation, designate managers to respond to governance template questions, and report performance results to the appropriate executive level in charge of organizational oversight. From preliminary conversations with nuclear operators, identifying a coordinator should not be a difficult task given that most organizations already have departments handling assessments and audits that are well-equipped to perform this function. Depending on the structure of a company, the governance template could be classified as a "standard" which would be implemented and evaluated within the Corporate Oversight and Audit division. Thus, it is imperative to understand how a

company or organization handles performance evaluations to determine whether the governance template can be easily incorporated.

Equally important is to identify the *owners* of the governance template, i.e., the individuals or groups responsible for addressing—and in essence, owning—the outcomes of the governance template process, including corrective actions that need to be addressed before the next review. Assigning an owner to each outcome ensures a level of accountability within the organization that the government template process is a serious effort meant to practice continuous improvement.

2. WORKFLOW AND INDEPENDENT ASSESSMENT OF IMPLEMENTATION

The coordinator will have to delineate how the governance template fits into existing workflows so that managers tasked to answer the governance template and "own" any corrective actions understand how this effort enhances their work. According to one nuclear operator, the ideal approach would be to select individuals along the leadership line—from the executive level to the division or site level—who would participate in a focus group to answer the governance template questions (for senior individuals, a one-on-one interview process may be more appropriate). For their circumstance, they would use the governance template to identify gaps and scenarios for improvement, i.e., instances where the focus group simply cannot answer a question (a gap), or clearly articulate why governance decisions are done a certain way (scenarios for improvement). The coordinator would then use a risk-based assessment to prioritize the identified gaps, such that the organization can triage what needs urgent attention and items that may have lower-risk, but could be easily executed. Through this triage process, the coordinator can then determine the organization's current state, or baseline, of security governance. To improve the current *state*, the coordinator would develop a plan with actionable, measurable, and results-oriented tasks for appropriate individuals or groups (hence, the "owners") to execute over a given timeline. The coordinator would issue a quarterly progress report to keep track of tasks and hold owners accountable. And as part of oversight, the coordinator would arrange an independent review in accordance to existing quality assurance procedures.

Clearly, this sample workflow and assessment plan would have to be modified to align with the requirements and preferences of a different facility. It is important to consider that executive structures, as well as managerial roles and responsibilities may vary not only for each company, but also each country. Given this variance, it is even more necessary to conduct a preliminary consultation as an opportunity to tailor the governance template accordingly.

3. BOARD INTERACTION

The governance template is tailored to gauge how decisions about security are made and relayed among the executive level of a given organization and company, including the Board. As seen in previous high-profile accidents like the Fukushima Daiichi meltdown, the public will scrutinize every mistake and demand accountability not only from the damaged facility, but the broader nuclear community.[31] As one nuclear operator put it, an accident or incident at any given facility will trigger public outrage or skepticism over safety and security in all facilities, even when there is no conceivable connection to the event. It is part of executive responsibility to clearly convey to relevant stakeholders including the public how operations are safe and secure to prevent a similar event happening at their facility.

Most organizations already have board members that closely follow corporate governance for security through their involvement with audit processes or oversight subcommittees that specifically handle security issues. Board members holding these roles could potentially review the governance template answers and communicate outcomes and progress to the wider board. Irrespective of the level of interaction the board will have with the governance template, the main goal is to encourage board members to reflect on their due diligence requirement for nuclear security, and the ways in which they demonstrate this obligation through action.

4. IMPACT ON OTHER WORKPLACE FUNCTIONS

Oftentimes, security oversight dovetails with other issue areas since managers are typically tasked multiple functions. In one case, a nuclear security manager at an organization also oversees the emergency preparedness and fire protection portfolios. Since there are overlapping elements among these issues, improving or expanding the oversight for security can engender positive outcomes for the other two. Indeed, several industry stakeholders have noted the positive externalities that the governance template could have in other areas; in reviewing the governance template questions, they are also compelled to think about how it would pertain to the other aspects of their business. Thus, it will be important for the governance template coordinator to consider these externalities prior to implementation.

ON THE HORIZON: EXPLORING SECURITY GOVERNANCE BEYOND NUCLEAR POWER

RESEARCH AND TEST REACTORS

Best practices and guidance for security are not as prevalent for research and test reactors (RTRs) compared to nuclear power plants. With 243 reactors operating in 55 countries, exploitable gaps in RTR security culture represent a unique, under-analyzed vulnerability, especially those still utilizing HEU fuel. Moreover, older RTRs, which represent a large share, were often built without the cyber and physical security considerations newer RTRs possess. Although IAEA guidance materials exist, RTR-specific nuclear security resources and publications are far from prolific; while individual RTR facilities' best practice documents are difficult to locate or nonexistent. Stimson's governance template presents an opportunity to assist RTR managers, operators, and researchers to implement and institutionalize a balance between the sometimes competing aims of safety, security, and research goals, often juggled by small staffs with numerous responsibilities and lacking in security experience and knowledge. Integrating these goals will help ensure RTRs can continue to create and retain the institutional knowledge necessary to continue their important work, without sacrificing security.

H. Mark Weidman Photography/ Alamy Stock Photo

NUCLEAR SUPPLIERS

The nuclear supply chain—reactors, turbines, equipment, fuel, etc.—is another area where the governance template may be of value. There may be opportunity to fold the governance template into existing compliance processes that nuclear suppliers already follow, such as nuclear-related regulations or export controls. In the context of an export control audit, the governance template could be used to supplement existing audit inquiries by adding a cybersecurity dimension. There are synergies between export control compliance and cybersecurity concerns, such as the need to keep controlled intangible technical data secure and access controlled/restricted. Further, manufacturers of equipment for nuclear power plants, such as control systems, can use the template to begin to incorporate cybersecurity functional into their products. The governance template could be of value in evaluating the effectiveness of that functionality—for both the manufacturer and the customer.

RADIOACTIVE SOURCES

Radiation sources and devices are used throughout the world and produced in many countries. Their wide range of applications include medical diagnostic and therapeutic procedures, agricultural pest eradication and food safety, industrial radiography, and oil and gas exploration. Many of these applications require mobile devices, such as radiography cameras to verify the integrity of welds during construction and well logging tools that make use of radioactive materials to chronicle characteristics in drilling oil and gas wells. Such devices regularly move from storage facilities, to transport vehicles, to job sites across the globe, but the architecture to govern their use remains weak. Thus, it is also worthwhile exploring the potential value of a radiological security-focused governance template for entities producing or using radioactive sources and devices as a non-traditional approach to enhancing global security. This work will begin by engaging with licensees and operators responsible for the stewardship of mobile radioactive devices.

CONCLUSION

Shaping Strong Security Norms Worldwide

While often unspoken, security is part of the bedrock upon which the nuclear enterprise sits and facilitates business. Stakeholders within the enterprise, especially industry, are expected to maintain the integrity of this foundation. Adopting security best practices is not a courtesy, but a *duty*—a crack in public confidence can jeopardize the future of "nuclear" as a viable and desirable energy and scientific resource. And as threats change and erode perceptions of what constitutes strong security practice, stakeholders will have to adjust accordingly to rebuild trust. Thus, demonstrating strong security is a continuous and constructive process. Those in charge must be attuned to political, technological, and economic trends that could exacerbate existing or create new threat vectors.

Recognizing that this is not an easy responsibility, the Stimson Center's proposed governance template serves as a practical resource to help define reasonable security practices for facilities by way of building common intent, understanding, and language across senior leadership making important security decisions. It aims to identify and archive what is currently being done, and most importantly, ***why*** it has been determined by management that this is the most appropriate course of action, and ***how*** this is communicated to the rest of the workforce. If an organization utilizes the governance template consistently, it will illuminate trends overtime of how reasonable security decisions have changed to address contemporary threats, and what has been most effective or what still needs improvement.

While the governance template has direct organizational value, it also has the potential to catalyze norm building around security governance on a larger scale. With enough organizations adopting the template, it could gradually institute an internationalized practice of maintaining a security governance and culture profile for any entity handling civilian nuclear and radiological material. To achieve this stage, all participants must believe in the underlying value in communicating and cultivating security culture, such that it becomes a widely accepted, if not expected, custom. As one nuclear specialist suggest, the governance template is a tool to encourage a habit of "holding one another to a higher standard." And in the same spirit, Stimson experts will continue to hone the template, updating when necessary, to ensure that the template is also up to the task.

ENDNOTES

[1] World Nuclear Association. “Reactor Database.” Facts and Figures. Accessed August 20, 2018. http://www.world-nuclear.org/information-library/facts-and-figures/reactor-database.aspx

[2] In the United States alone, there are 14 premature power plant closures, 10 of which are due to steep market competition. Bill Pitesa, Leadership During Times of Change (presentation at the International Conference on Quality, Leadership and Management in the Nuclear Industry, Ottawa, Canada, July 18, 2018). ; IAEA. “Energy, Electricity and Nuclear Power Estimates for the Period up to 2050.” Reference Data Series No. 1 2017. Accessed August 20, 2018. https://www-pub.iaea.org/MTCD/Publications/PDF/17-28911_RDS-1%202017_web.pdf

[3] International Atomic Energy Agency. “Nuclear Power and the Paris Peace Agreement.” Accessed August 20, 2018. https://www.iaea.org/sites/default/files/16/11/np-parisagreement.pdf

[4] IBM. “Cost of a Data Breach Study.” Security Study by Ponemon. Accessed August 20, 2018. https://www.ibm.com/security/data-breach

[5] Condliffe, Jaime, “The number of cyber incidents doubled in 2017,” The Technology Review, January 26, 2018, accessed August 20, 2018. https://www.technologyreview.com/the-download/610074/the-number-of-cyber-incidents-doubled-in-2017/ ; Online Trust Alliance, “Cyber Incidents and Breach Trends Reports: Review and Analysis of 2017 Cyber Incidents, Trends, and Key Issues to Address,” January 25, 2018, Accessed October 15, 2018, https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.

[6] Symantec. “Ransom Wannacry.” Security Center. Last modified May 24, 2017. Accessed August 20, 2018. https://www.symantec.com/security-center/writeup/2017-051310-3522-99; Karan Sood and Shaun Hurley, “NotPetya Technical Analysis—A Triple Threat: File Encryption, MFT Encryption, Credential Theft,” Crowdstrike, June 29, 2017, accessed August 20, 2018, https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ ; Department of Homeland Security. “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” United States Computer Emergency Readiness Team. Last modified March 16, 2018. Accessed August 20, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A

[7] IBM. “IBM X-Force Threat Intelligence Index 2017.” Security Intelligence. Last modified March 29, 2017. Accessed August 20, 2018. https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/

[8] ICF International. “Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.” Accessed August 20, 2018. https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf ;The President’s National Infrastructure Advisory Council. “Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.” (Washington D.C.: National Infrastructure Advisory Council, 2017) https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

[9] Olmstead, Kenneth and Aaron Smith. “Americans and Cybersecurity.” Pew Research Center, January 26, 2017. Accessed on August 20, 2018. https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

[10] Veltsos, Christophe, “Lessons from the Marsh ‘Global Cyber Risk Perception Survey’: Disconnects Persist Despite Increased Executive Involvement,” Security Intelligence, April 18, 2018, accessed August 20, 2018. https://securityintelligence.com/lessons-from-the-marsh-global-cyber-risk-perception-survey-disconnects-persist-despite-increased-executive-involvement/; Marsh. “By the Numbers: Global Cyber Risk Perception Survey.” Accessed August 20, 2018. https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Microsoft%20Global%20Cyber%20Risk%20Perception%20Survey%20February%202018.pdf

[11] The Nuclear Energy Institute. “Working Group 1 Report: Managing Cyber Threats.” Nuclear Industry Summit 2016. Accessed August 20, 2018. http://nis2016.org/wp-content/uploads/2016/02/Working-Group-1-Report-Managing-Cyber-Threats.pdf

[12] IAEA. “Self-assessment of Nuclear Security Culture in Facilities and Activities.” IAEA Nuclear Security Series No. 28-T 2017. Accessed August 20, 2018. https://www-pub.iaea.org/books/iaeabooks/10983/Self-assessment-of-Nuclear-Security-Culture-in-Facilities-and-Activities

[13] World Institute for Nuclear Security. “Corporate Governance Arrangements for Nuclear Security.” Accessed on August 20, 2018. https://wins.org/document/corporate-governance-arrangements-for-nuclear-security/

[14] Mark Fabro, “Updating Threat Model: Using Past Assessment and Incident Analysis to Predict Cyber Attributes and Characteristics of the Adversary”(presentation at the International Conference on Quality, Leadership and Management in the Nuclear Industry, Ottawa, Canada, July 18, 2018).

[15] IAEA. "Amendment to the Convention of the Physical Protection of Nuclear Material." Information Circular. Accessed August 20, 2018. https://www.iaea.org/sites/default/files/infcirc274r1m1.pdf

[16] IAEA. "Self-Assessment of Nuclear Security Culture in Facilities and Activities." IAEA Nuclear Security Series No. 28-T 2017. Accessed on August 20, 2018. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf

[17] Lovely Umayam, Kathryn Rauhut, and Jacqueline Kempfer. "Lifting the Lid on Nuclear Liability." Stimson Center, 2018. Accessed August 20, 2018. https://www.stimson.org/sites/default/files/file-attachments/LiftingTheLid-R4-WEB.pdf

[18] Alexandra Van Dine, Michael Assante, and Page Stoutland, Ph.D. "Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities." Nuclear Threat Initiative, 2016. Accessed August 20, 2018. http://www.nti.org/media/documents/NTI_CyberThreats__FINAL.pdf ; Caroline Baylon, Roger Brunt, and David Livingstone. "Cyber Security at Civil Nuclear Facilities: Understanding the Risks." Chatham House, September 2015. Accessed on August 20, 2018. https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf; In January 2003, the Davis-Besse Nuclear Power Plant saw its private network become infected with the slammer worm, a prolific computer worm that drastically slowed down computers, resulting in a safety monitoring system being disabled for nearly five hours despite employees' belief it was protected by a firewall. In April 2016, it was discovered that the Gundremmingen nuclear power plant, located in Germany, had been infected with multiple computer viruses, despite its lack of connection to the internet, through the use of malware-infested removable data drives.

[19] Occidental College. "BLYTH v. BIRMINGHAM WATERWORKS CO." Accessed on August 20, 2018. https://sites.oxy.edu/whitney/xaccess/ec357/cases/tort/blyth_v_birmingham.html

[20] Decker, Debra and Kathryn Rauhut. "So You Think Nuclear Plant Liabilities Are Covered?" Stimson Center, April 21, 2017. Accessed on August 20, 2018. https://www.stimson.org/content/so-you-think-nuclear-plant-liabilities-are-covered

[21] Decker, Debra and Kathryn Rauhut. "Cyber Risks Go Nuclear." Stimson Center, August 10, 2018. Accessed on August 20, 2018. https://www.stimson.org/content/cyber-risks-go-nuclear

[22] Nicole Perlroth and David E. Sanger, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," New York Times, March 15, 2018, accessed August 20, 2018. https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

[23] Kern, Rebecca, "Energy Officer Not Confident Utilities Prepared for Cyberattacks." Bloomberg Environment, September 27, 2018; https://bnanews.bna.com/environment-and-energy/energy-official-not-confident-utilities-prepared-for-cyberattacks/; U.S. House of Representatives, Committee on Energy and Commerce, Testimony of Assistant Secretary Keren Evans, Office of Cybersecurity, Energy Security, and Emergency Response, September 27, 2018. https://docs.house.gov/meetings/IF/IF03/20180927/108725/HHRG-115-IF03-Wstate-EvansK-20180927.pdf.

[24] Justia. "The Tj Hooper, 60 F.2d 737 (2d Cir. 1932)." Accessed on August 20, 2018. https://law.justia.com/cases/federal/appellate-courts/F2/60/737/1542549/

[25] FindLaw. "IN RE: WORLD TRADE CENTER BOMBING LITIGATION." Accessed on August 20, 2018. https://caselaw.findlaw.com/ny-supreme-court/1143026.html

[26] Justia. "In Re Air Disaster at Lockerbie Scotland on December 21, 1988.judith A. Pagnucco, Individually and As Executrix of t he estate of Robert I. Pagnucco, Deceased; Molena A. Porter, individually and As Administratrix of the Estate of Walter l. Porter, Deceased and Dona Bardelli Bainbridge, individually and As Administratrix of the Estate of Harry M. Bainbridge, Plaintiffs-appellees, v. Pan American World Airways, Inc., and Alert Management Systems, Inc., Defendants-appellants, 37 F.3d 804 (2d Cir. 1992)." Accessed on August 20, 2018. https://law.justia.com/cases/federal/appellate-courts/F3/37/804/508796/

[27] Eric Chien, "Perspective on the Cyber Threat" (presented at the Stimson Center Nuclear Security Roundtable: Forging Strong Security Norms: The Value of "Due Care" in Nuclear Facilities, London, May 22, 2018).

[28] Ibid.

[29] Maxey, Levi. "Jumping the Air Gap: How to Breach Isolated Networks." The Cipher Brief, March 26, 2017. Accessed August 20, 2018. https://www.thecipherbrief.com/jumping-the-air-gap-how-to-breach-isolated-networks

[30] Stimson Center. "Nuclear Security Governance Template." Accessed on August 20, 2018. https://www.stimson.org/nucleargovernance

[31] Jake Adelstein. "Who's responsible for the Fukushima Disaster?" Japan Times, October 3, 2015, Accessed October 11, 2018, https://www.japantimes.co.jp/news/2015/10/03/national/media-national/whos-responsible-fukushima-disaster/#.W8AaR_5KhXg. ; Mina Pollmann, "3 TEPCO Execs To Face Trial for Fukushima Nuclear Disaster" The Diplomat, March 1, 2016, Accessed October 11, 2018, https://thediplomat.com/2016/03/3-tepco-execs-to-face-trial-for-fukushima-nuclear-disaster/

ABOUT THE AUTHORS

MARIA LOVELY UMAYAM

Umayam is a Research Analyst and Program Manager for Stimson Center's Nuclear Security Program. Her work focuses on innovative ways to promote and incentivize WMD nonproliferation at the multilateral, national, and operational levels. At Stimson, she also leads the Security and Trade Efficiency Platform (STEP) project, which examines the intersection between WMD nonproliferation and global trade development. Prior to joining Stimson, Lovely served as a Program Manager at the Office of Nonproliferation and Arms Control within the U.S. Department of Energy—National Nuclear Security Administration (DOE/NNSA), where she implemented nuclear safeguards engagement projects in Southeast Asia and Latin America. At DOE/NNSA, she also helped coordinate nonproliferation and nuclear-stability focused Track 1.5 engagements in South Asia and Southeast Asia. She has presented her research at the International Atomic Energy Agency, the Organisation for the Prohibition of Chemical Weapons, as well as government-sponsored convenings.

JACKIE KEMPFER

Kempfer is a Research Associate with the Nuclear Security program at the Stimson Center. She holds a Masters of International Studies from North Carolina State University, where she concentrated on nuclear security and nonproliferation. She also holds a Bachelor of Arts in History from East Carolina University. She is currently working with the private sector to generate ideas that incentivize the development and adoption of stronger, comprehensive nuclear security standards among industry stakeholders to reduce the risk posed by nuclear terrorism. She is a member of the Institute of Nuclear Materials Management, North East Chapter Executive Committee.

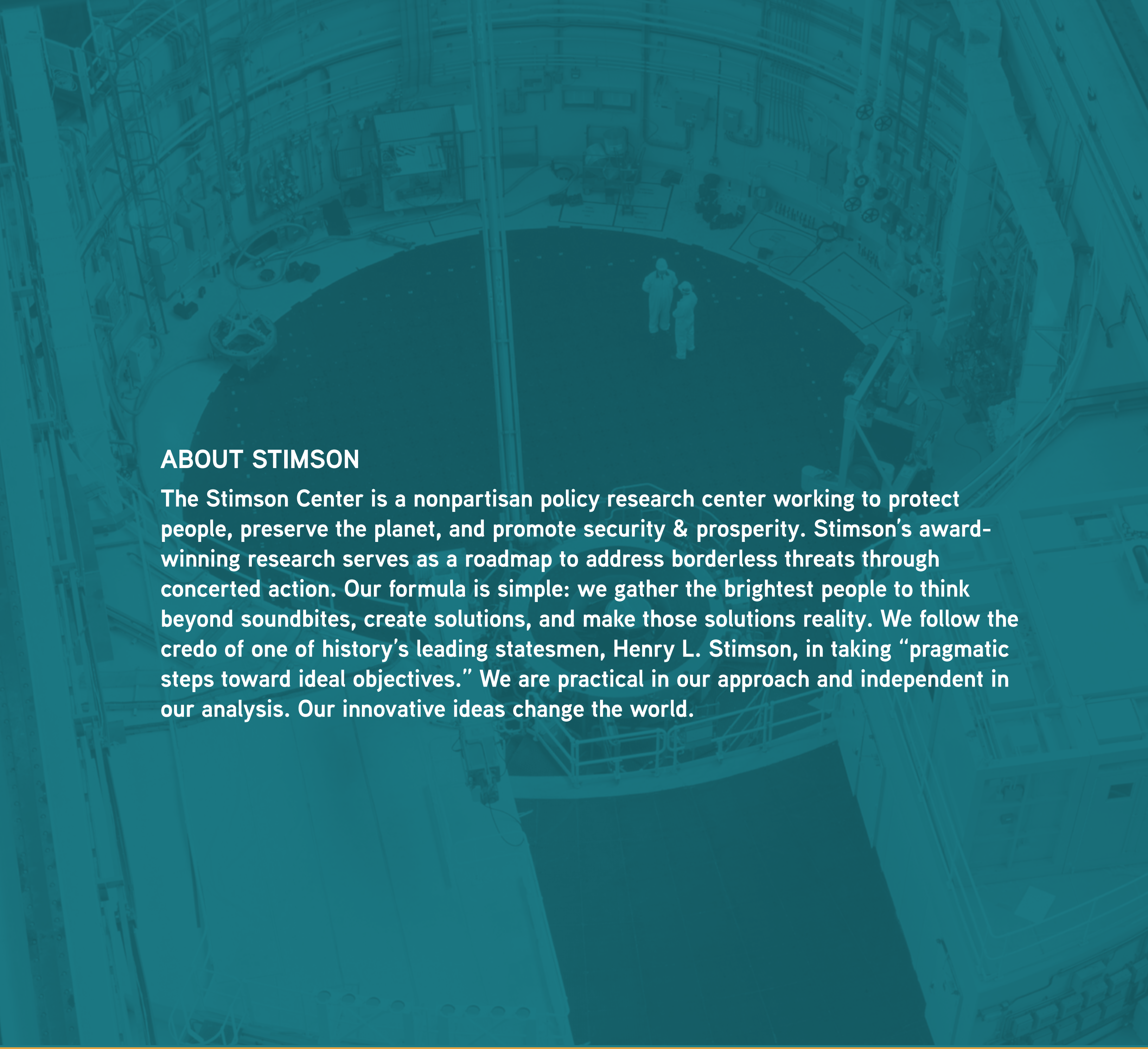
KATHRYN RAUHUT

Rauhut is a Stimson Center Non-resident Fellow and an attorney specializing in international security based in Vienna, Austria. She works primarily on nuclear security governance, accountability and liability issues with a focus on cybersecurity. Prior to her work with the Stimson Center's Managing Across Boundaries initiative, she was a Strategic Advisor to the Internet Security Alliance and to the World Institute for Nuclear Security (WINS). In her role at WINS, Rauhut led international roundtables and authored policy papers on improving global governance of nuclear and cybersecurity through building the business value of security. Previously, she was the Deputy General Counsel of Lawrence Livermore National Laboratory in California. She is a member of the California Bar Association, the American Bar Association, and the International Nuclear Lawyer's Association.

ACKNOWLEDGEMENTS

The three years of research consisting of in-person interviews, cross-sector roundtables, and publications would not be possible without the generous support from the MacArthur Foundation, the Carnegie Corporation, and the U.S. Department of State—Partnership for Nuclear Threat Reduction. We are also grateful for the continued collaboration with the World Institute for Nuclear Security (WINS), especially for their willingness to build on their initial governance template draft.

This body of work would not exist without the time, attention, and insights from stakeholders across the nuclear enterprise who have attended Stimson's nuclear security events. Their openness to explain their on-the-ground perspectives, brainstorm ideas, and provide candid feedback helped shape the current iteration of the template. We give special thanks to Debra Decker, Ray Biagini, Kevin Cuddy, Lisa Clarke, Terry Young, Stephen Tromans, Ian Truman, Eric Chien and Don Dudenhoeffer for offering their expertise, which deeply informed our research on tort liability and cybersecurity. Lastly, we are grateful for the assistance provided by Jared Zimmerman and Christopher Eli Enos for completing this report.



ABOUT STIMSON

The Stimson Center is a nonpartisan policy research center working to protect people, preserve the planet, and promote security & prosperity. Stimson's award-winning research serves as a roadmap to address borderless threats through concerted action. Our formula is simple: we gather the brightest people to think beyond soundbites, create solutions, and make those solutions reality. We follow the credo of one of history's leading statesmen, Henry L. Stimson, in taking "pragmatic steps toward ideal objectives." We are practical in our approach and independent in our analysis. Our innovative ideas change the world.

STIMSON

STIMSON.ORG