Systems of Cyber Resilience: Electricity Initiative

WORLD ECONOMIC FORUM

Response to the White House's Request on Harmonizing Cybersecurity Regulations

WHITE PAPER

OCTOBER 2023

Images: Getty Images

Contents

Executive summary 3

1 About the Systems of Cyber Resilience: Electricity Initiative 4

2 The Global Regulations Working Group 5

3 The White House request for information on cybersecurity regulatory harmonization 6

- 3.1 Conflicting international cybersecurity requirements 7
- 3.2 Sector to prioritize for regulatory harmonization 8
- 3.3 International dialogues on harmonization 9
- 3.4 Ongoing international initiatives 10
- 3.5 Regulatory reciprocity examples 11

Conclusion 12

Contributors 13

Annex 1: Related publications 15

Endnotes 16

Executive summary

On 19 July 2023, the White House Office of the National Cyber Director (ONCD) of the United States (US) issued a request for information (RFI)[1] about harmonizing cybersecurity regulations globally and ensuring regulatory reciprocity between countries. This RFI is an extension of the goals outlined in the US National Cybersecurity Strategy,[2] which aims to synchronize not just regulations and guidelines but also the evaluation and inspection processes for regulated entities. It marks progress on one of the 69 initiatives unveiled in July as part of the US National Cybersecurity Strategy Implementation Plan.

In September 2022, the World Economic Forum Systems of Cyber Resilience: Electricity Initiative (SCRE) community[3] had identified global regulatory interoperability as one of its key focus areas, and had set up the Global Regulations Working Group to facilitate interoperability of global cyber regulations in the electricity sector.

This working group tackles the challenges of complex, industry and sector agnostic, fragmented, inconsistent, and sometimes conflicting regulations. These siloed regulations lack and prevent interoperability, resulting in increased costs and inefficiencies as limited resources are diverted to address compliance challenges instead of directly addressing sectorial and organizational cybersecurity posture.

Given SCRE's unique global vantage and expertise as well as its ongoing work on this topic, the community has come together to produce this white paper to answer questions in the international section (Section 9) of the RFI. This section addresses cybersecurity requirement conflicts, priority sectors and regions, international dialogues, ongoing international initiatives and regulatory reciprocity.

The SCRE community welcomes and supports ONCD's regulatory harmonization effort. Its recommendations for the ONCD are as follows:

- Continue ONCD's ongoing efforts to increase global regulatory interoperability, increase security and reduce costs.
- Prioritize security over compliance by adopting a risk-based approach.
- Engage private, public and civil society stakeholders from the earliest stages of the policy and regulatory processes.
- Leverage existing international technical standards established by non-government bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- Participate in international dialogues and international initiatives on cybersecurity.

1 About the Systems of Cyber Resilience: Electricity Initiative

Since 2018, the World Economic Forum's Systems of Cyber Resilience: Electricity Initiative (SCRE) has brought together global leaders from more than 60 electricity utilities, energy services companies, regulators and other relevant organizations, to collaborate and develop a clear and coherent global cybersecurity vision for the electricity ecosystem.

SCRE is the only global, electricity-industry specific, multistakeholder public-private partnership where cybersecurity leaders collaborate and improve ecosystem-wide cyber resilience in the electricity sector.

> **This initiative provides a forum for global electric companies and premier industry partners to take the lead in driving increased maturity and capability to address cyber threats all nations are facing.**
>
> Tom Wilson, Senior Vice-President and Chief Information Security Officer, Southern Company, USA

2 The Global Regulations Working Group

Regulatory interoperability is one of the key focus areas of the SCRE and its Global Regulations Working Group.

The working group addresses the complexities of regulatory challenges that span across the electricity sector, characterized by fragmentation, inconsistency and occasional conflicts. These regulatory hurdles hinder the achievement of global interoperability, leading to heightened costs, inefficiencies and missed opportunities as resources are redirected to tackle regulatory issues rather than enhancing sector-specific and organizational cybersecurity postures. The key insights of the working group have been:

1. The evolution of the cyber threat landscape has led to an increase in cybersecurity regulations globally.
2. Global regulations are fragmented and, in some cases, conflicting, which increases costs and inefficiencies and impacts cybersecurity through the opportunity costs of diverting limited resources.
3. Organizations have had to take hard, risk-based approaches ranging from managing regulatory complexities to exiting certain markets.
4. Regulations need to prioritize security over compliance by adopting a risk-based approach.

The working group has taken the following positions on the key global regulatory themes identified:

1. **Compliance and enforcement:** Global commitment to prioritize security over compliance.
2. **Data protection and privacy:** Global commitment to support data protection and privacy regulations such as the General Data Protection Regulation (GDPR) of the European Union (EU).
3. **Information sharing:** Global commitment to create and use a common information-sharing protocol and taxonomy worldwide, and to support the respective electricity information sharing and analysis centres (ISACs).
4. **Incident response and reporting:** Global commitment to adopt a common and efficient international incident reporting taxonomy and requirements.
5. **Cybersecurity hygiene internal policies and procedures:** Global commitment to establish basic cyber hygiene principles specific to the electricity sector.
6. **Penetration testing:** Global commitment to regular internal penetration testing which includes operational technology (OT) penetration testing.
7. **Vulnerability disclosure and management:** Global commitment to sectorial disclosure of vulnerability among closed groups of sector-specific, pre-authorized entities.
8. **Risk assessment and management:** Global commitment to applying risk assessment methodology consistently across both information technology and operational technology environments.
9. **Third-party risk management:** Global commitment that every organization in the supply chain must consider and be responsible for the cybersecurity of its scope of work.
10. **Adoption of existing international standards versus creation of unique, national (or regional) standards:** Global commitment to adoption of existing international standards that are mature such as ISO 27001 and IEC 62443.

The working group will further elaborate these positions and is scheduled to publish a “Facilitating Global Interoperability of Cyber Regulation in the Electricity Sector” paper on 15 November 2023.

3 The White House request for information on cybersecurity regulatory harmonization

On 19 July 2023, the White House Office of the National Cyber Director (ONCD) announced a request for information (RFI) on cybersecurity regulatory harmonization and regulatory reciprocity. The RFI builds on the commitments made in the White House National Cybersecurity Strategy to "harmonize not only regulations and rules, but also assessments and audits of regulated entities." The RFI advances one of the 69 initiatives that the United States National Cybersecurity Strategy Implementation Plan announced in July.

Given the SCRE's unique global perspective and proficiency in this field, the community has shared its collective knowledge in this white paper. The aim is to provide precise responses to inquiries in the international section (Section 9) of the RFI stated below:

> **9. International – Many regulated entities within the United States operate internationally. In a recent report from the President's National Security Telecommunications Advisory Council (NSTAC), the NSTAC noted that foreign governments have been implementing regulatory regimes with "overlapping, redundant or inconsistent requirements…"**
>
> Fact Sheet: Office of the National Cyber Director Requests Public Comment on Harmonizing Cybersecurity Regulations – Request for Information on Cyber Regulatory Harmonization

A. Identify specific instances in which US federal cybersecurity requirements conflict with foreign government cybersecurity requirements.

B. Are there specific countries or sectors that should be prioritized in considering harmonizing cybersecurity requirements internationally?

C. Which international dialogues are engaged in work on harmonizing or aligning cybersecurity requirements? Which would be the most promising venues to pursue such alignment?

D. Please identify any ongoing initiatives by international standards organizations, trade groups or non-governmental organizations that are engaged in international cybersecurity standardization activities relevant to regulatory purposes. Describe the nature of those activities. Please identify any examples of regulatory reciprocity within a foreign country.

E. Please identify any examples of regulatory reciprocity between foreign countries or between a foreign country and the United States.

3.1 A. Conflicting international cybersecurity requirements

Identify specific instances in which US federal cybersecurity requirements conflict with foreign government cybersecurity requirements.

Government agencies worldwide that create cybersecurity requirements for industry, including those of the US, frequently adopt distinct approaches to address identical or similar sets of cybersecurity challenges due to the absence of a global consensus. This leads to complex, industry and sector agnostic, fragmented, inconsistent and sometimes conflicting regulations, which lack and prevent mutual interoperability.

The evolution of the cybersecurity threat landscape and regulators' reflexive response to tighten regulations exacerbates the problem. Organizations are forced to divert limited resources to address regulatory compliance challenges instead of focusing on their cybersecurity posture. In addition to a lack of consensus on cyber requirements, a lack of consensus exists on who or what is in the scope of these regulations (e.g. varying critical infrastructure sector designations, different regulations bringing various systems into scope, etc.)

Today's digital economy transcends national boundaries, requiring robust and unified international cybersecurity standards to ensure that multinational companies are best equipped to respond to new threats by malicious actors as they arise.

As such, businesses around the world look to standards set by non-government bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for guidance on a broad range of cybersecurity issues and as benchmarks for global best practices. When different regulators use widely recognized international technical standards – such as the ISO/IEC 27000 series of information security controls and the IEC 62443 series of industrial control system controls—to inform their policies, it not only sets a high standard of security for companies to adhere to but also lowers costs and assures interoperability with other regulatory regimes.

Conversely, when different regulators and policy-makers use their own local standards and laws as a reference for establishing cybersecurity requirements, it contributes to the growing fragmentation of the global digital policy landscape, in turn unduly raising compliance costs for multi-jurisdictional companies and diverting resources from sound cyber-risk management activities.

The current siloed approach to cybersecurity regulation has not led to a more secure global digital economy. It is well known from the Prisoner's Dilemma problem in game theory that stakeholder cooperation on cybersecurity regulations will increase security of the global digital economy. However, the inherent challenge has always been: who will move first? It is imperative to resolve and make progress on this cooperation issue.

Examples of diverging cybersecurity regulations can be found in national cybersecurity labelling programmes such as those of the US, EU and Singapore. As more and more products released in the market require internet connectivity, the surface area of cyber risks to consumers has increased tremendously. To address this concern, several governments have announced plans to develop their own cybersecurity labelling schemes. For example, Singapore's Cyber Security Agency first launched its Cybersecurity Labelling Scheme (CLS)[4] in 2020 to set security rating levels that buyers of smart devices could use to make informed choices. In September 2022, the EU proposed its Cyber Resilience Act[5] to establish common security standards for products with digital elements connected to a device or network in EU member-states. And lastly, in June 2023, the Biden administration announced a new US Cyber Trust Mark[6] programme to be led by the Federal Communications Commission with very similar elements to the Singaporean and European models.

These three cyber labelling initiatives share the common goal of providing assurance to consumers that the products they purchase are equipped with adequate safeguards to protect them from cyber harms, but they have different scopes and specific requirements. Recognizing sectoral and jurisdictional nuances in the threat landscape, the most sensible approach in developing these national cybersecurity labels is to base them in international consensus-based technical standards so as to ensure maximum interoperability.

The SCRE community welcomes and supports the regulatory harmonization effort by the ONCD and recommends that they continue their efforts towards global regulatory harmonization to increase interoperability, enhance security and reduce costs.

3.2 B. Sector to prioritize for regulatory harmonization

Are there specific countries or sectors that should be prioritized in considering harmonizing cybersecurity requirements internationally?

Sector: Electricity

Cybersecurity has become increasingly important in the electricity sector. Several converging trends contribute to an escalating risk environment: digitized, networked devices now permeate energy infrastructure; attacks on infrastructure have escalated; the energy transition is shifting the sector away from the historic business models that regulations take for granted; an internet of things (IoT) composed of networked consumer and industrial devices bridges physical and digital realms; and artificial intelligence (AI) offers new and powerful capabilities to defenders as well as attackers.

Electrical infrastructure is critical infrastructure. Without reliable electricity generation, transmission and distribution, other parts of the economy cannot function.

> The SCRE community highlights the electricity sector as a sector to prioritize for achieving interoperability of cybersecurity requirements internationally.

Digitization has made electrical infrastructure more efficient while lowering its carbon intensity. Renewable energy technologies cannot function without digital management to smoothen variable inputs. Many future technologies, business models and elements of public infrastructure rely on digitized equipment, including electric vehicles, distributed generation and smart cities. At the same time, networked, digital equipment is relatively new. Cybersecurity practices across the industry are not uniformly mature. The interconnected nature of the US electric grid means that the consequences of a successful cyberattack on one part of the grid could propagate across the entire physical infrastructure.

Attacks against the electricity sector continue to escalate. Federal agencies have repeatedly identified persistent, sophisticated threats that have penetrated electricity sector organizations, sometimes without those organizations becoming aware that they have been compromised. Some of these attacks have been attributed to groups with nation-state backing. In August 2023, the International Energy Agency reported that cyberattacks on utilities had more than doubled from 2020 to 2022.[7] Surveys of cybersecurity professionals likewise show increased concern about cyberattacks targeting industrial control systems – such as those operating the electricity infrastructure in countries including the US.[8]

Government agencies that create cybersecurity requirements for industry in the US and elsewhere have not kept pace with changes in the energy sector. For example, federal regulations in the US electricity sector focus on bulk distribution. This was appropriate in an era when large, centralized generation was the dominant business model. As renewable energy grows, these assumptions must be revisited. Likewise, differing cybersecurity reporting requirements apply to US natural gas infrastructure and US electricity infrastructure — yet these systems are intrinsically linked, with natural gas providing the single largest source of energy to the electricity sector.

Further change is already underway in the electricity sector. AI offers new capabilities that will be appealing to attackers and essential to defenders. AI enables cybersecurity monitoring that can detect and respond to attacks with machine-like speeds, but it remains unclear how regulatory regimes will embrace or constrain AI in infrastructure. Generative AI is likely to be abused by attackers seeking to craft more effective attacks — potentially producing more believable phishing attacks, bypassing malware signature detection or lowering the skill required to translate malicious intent into action.

The EU has by far been the most active in proposing and advancing legislation and regulations for emerging technologies and, as such, has become a de-facto standard setter for digital policy, as illustrated by the widespread adoption of data protection laws modelled after the GDPR. The US should use every avenue of dialogue and cooperation to encourage and support the EU to align its policies more closely to widely recognized technical standards based on international consensus (while also ensuring that US domestic policies are grounded in international consensus-based technical standards).

For example, the newly proposed Cyber Resilience Act of the EU made no reference to international standards. On the contrary, the EU mandated the European standards organizations to develop European harmonized standards to demonstrate compliance with the Cyber Resilience Act. This regionalization of cybersecurity standards defies the consensus on the need for international standards and intensifies the burden on global companies by forcing them to conform to multiple assessments in different markets. In response, the US should work through bilateral and multilateral fora to encourage European alignment with international standards to safeguard the global competitiveness of industries and protect the attractiveness of the European market.

The US, EU and other jurisdictions can work towards mutual recognition of cybersecurity requirements. Nuances in different jurisdictions understandably create different priorities for policy-makers to manage and legislate. Nevertheless, local nuance need not render two

sets of cybersecurity requirements incompatible. Cybersecurity standards should be interoperable across jurisdictions, with a baseline level of trust. As the internet knows no borders, jurisdiction-specific cybersecurity standards without cross-border interoperability and mutual recognition are counterintuitive and counterproductive.

3.3 C. International dialogues on harmonization

Which international dialogues are engaged in work on harmonizing or aligning cybersecurity requirements? Which would be the most promising venues to pursue such alignment?

> The SCRE community encourages policy-makers and regulators to participate in international dialogues on cybersecurity to improve the cross-border interoperability of regulations, which can enhance security and lower costs.

The EU-US Cyber Dialogue[9]

The EU-US Cyber Dialogue is an encouraging forum, but it is unclear how effective or successful it has been. Between 2014 and 2022, the EU and the US have held eight cyber dialogues to address and coordinate on cybersecurity issues, foster international collaboration and mutual understanding, and make cybersecurity practices more consistent across the two jurisdictions. The maturity of this dialogue makes it a promising venue for promoting greater alignment on cybersecurity policy, though its current track record doesn't show much visible progress. Both jurisdictions should take advantage of this platform to find common ground to reach their cybersecurity objectives and base their respective policy agendas on international standards such as the ISO/IEC 27000 and IEC 62443 series.

US-Japan Cyber Dialogue[10]

On 1 May 2023, Tokyo played host to the 8th Japan-US Cyber Dialogue, a significant event aimed at aligning international cyber policies and strengthening cybersecurity measures between the two countries. Various ministries and agencies took part, focusing on extensive discussions on bilateral operational cybersecurity cooperation, domestic cyber policies, and Japan-US cooperation on cyber issues, including those of regional and international significance. The platform enabled the exchange of information on cyber threats and deliberations on cyber defence and security collaboration. It played a pivotal role in deepening bilateral cooperation.

The two sides agreed to amplify domestic cybersecurity measures through a comprehensive whole-of-government approach, underlining the criticality of Japan-US collaboration in combating cyber threats.

France-United Kingdom Cyber Dialogue[11]

France and the United Kingdom held their fourth cyber dialogue in Paris on 11 May 2023. Both countries reiterated their commitment to collaborate in the field of cyberspace to promote security and stability in an inclusive, non-fragmented and secure cyberspace. They discussed their analysis of the threat and shared the latest developments in their respective cybersecurity policies. The two countries also talked about their priorities for ongoing discussions in various multilateral fora and discussed the implementation of a joint initiative to address the threat from commercial cyber proliferation. Additionally, they discussed the strengthening of bilateral coordination in response to cyber threats.

3.4 D. Ongoing international initiatives

Please identify any ongoing initiatives by international standards organizations, trade groups or non-governmental organizations that are engaged in international cybersecurity standardization activities relevant to regulatory purposes. Describe the nature of those activities. Please identify any examples of regulatory reciprocity within a foreign country.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

The ISO and IEC are the world's leading standard-setting bodies. While the ISO oversees standards development across a wide variety of industries, the IEC specializes in standardizing sectors related to electrical, electronic and related technologies. Each has a well-established track record for defining industry norms and benchmarks that are used by companies around the world.

The ISO/IEC 27000 series and the IEC 62443 series are both examples of cybersecurity standards that encompass a broad range of controls related to, among other topics, privacy protection, monitoring and evaluation, risk management and cloud services controls. Currently, the ISO and IEC are developing a Universal Cybersecurity Labelling Framework (ISO/IEC 27404)[12] "for the development and implementation of cybersecurity labelling programs for consumer IoT products".

Given the global recognition and use of ISO/IEC standards, the US should encourage and play an active role in the development of ISO/IEC 27404, particularly with the aim of reducing divergence from the widely used IoT security standards ETSI EN 303 645[13] and NIST 8425,[14] the key standards referenced for the overwhelming majority of IoT device requirements across the world.

European Union Agency for Cybersecurity (ENISA)[15]

ENISA plays a significant role in shaping cybersecurity regulations and policies in the EU. It contributes to the EU's cyber policy by enhancing the trustworthiness of information and communications technology (ICT) products, services and processes through cybersecurity certification schemes. In addition, ENISA provides guidelines and recommendations for various sectors, including for critical infrastructure, cloud computing and IoT.

Internet Engineering Task Force (IETF)[16]

IETF is a large, open, international community of network designers, operators, vendors and researchers, and is working on technical and operational internet standards. These standards often include protocols and frameworks that enhance cybersecurity measures, such as encryption, authentication and network security. Regulatory bodies and organizations often refer to IETF standards when formulating cybersecurity regulations, as they are widely recognized and trusted in the industry. IETF also collaborates with other organizations and stakeholders to address cybersecurity challenges and develop solutions to ensure a secure and resilient internet infrastructure.

Connectivity Standards Alliance (CSA)[17]

CSA is an international collaborative of companies that develops, publishes and maintains universal open standards for devices. For example, the CSA created the Matter standard[18] for interoperability of smart home and IoT devices.

As countries around the world begin to develop and launch cybersecurity labels, CSA has been proactively engaging with governments and has found considerable overlap between different country requirements. As such, CSA aims to minimize the compliance burden for manufacturers and offer a single certification programme that encompasses all security standards required by different country regimes, whether mandatory or voluntary. CSA has been coordinating with the US government to ensure that certifying companies to CSA's single certification programme will make them eligible for the US Cyber Trust Mark. It is important that the US government continues to engage with CSA as a partner for rolling out the US Cyber Trust Mark, and also encourages other countries to engage with CSA and similar entities so as to streamline cyber labelling requirements for companies and consumers alike.

SCRE initiative

The World Economic Forum's SCRE initiative is the only global, electricity-industry specific, multistakeholder public-private partnership where cybersecurity leaders from across the industry come together to improve the cyber resilience of the electricity sector. Since 2018, SCRE has engaged global leaders from more than 60 electricity utilities, energy services companies, regulators and other relevant organizations, to collaborate and develop a clear and coherent global cybersecurity vision for the electricity ecosystem.

> **The SCRE community recommends that policy-makers and regulators participate in international initiatives on cybersecurity and build on existing international technical standards issued by non-government bodies such as the ISO and the IEC.**

SCRE's Global Regulations Working Group

Regulatory interoperability is one of SCRE's key focus areas. Its Global Regulations Working Group is working towards facilitating interoperability of global cyber regulations in the electricity sector, which is a complex sector where regulations are often fragmented, inconsistent and conflicting. This lack of global interoperability increases costs and inefficiencies and impacts the sectorial and organizational cybersecurity posture.

3.5 E. Regulatory reciprocity examples

Please identify any examples of regulatory reciprocity between foreign countries or between a foreign country and the United States.

EU-US Data Privacy Framework[19]

On 10 July 2023, the European Commission ratified an adequacy decision pertaining to the EU-US Data Privacy Framework, affirming that the US upholds a data protection standard on par with that of the EU. This decision essentially permits the secure transfer of personal data from the EU to US companies engaged in the Data Privacy Framework, eliminating the need for supplementary transfer precautions.

Singapore Cybersecurity Labelling Scheme

Following the release of the Singapore Cybersecurity Labelling Scheme in 2020, Singapore has signed two regulatory reciprocity agreements regarding cybersecurity labels. In 2021, Singapore signed a memorandum of understanding with Finland to mutually recognize the cyber labels developed by the CSA and the Transport and Communications Agency of Finland (Traficom). In 2022, the Singapore Cyber Security Agency and the Federal Office for Information Security of Germany (BSI) similarly agreed on mutual recognition of labels. The Singapore-Finland MoU provides mutual recognition for products with a rating of CLS Level 3 and above, whereas the Singapore-Germany agreement does so for products with a rating of CLS Level 2 and above.

US Food and Drug Administration (FDA) Systems Recognition[20]

The FDA has developed a collaborative system with international regulatory agencies to promote and streamline comparable regulatory programmes. The collaboration is called Systems Recognition (SR), and SR processes create an optional system for assessing each other's food safety systems.

The FDA has signed SR agreements with Canada, Australia and New Zealand. Although not mandatory for importing goods into the United States, these agreements are designed to improve efficiency and highlight regulatory priorities. The SR process includes an in-country verification framework using the FDA's in-country assessment tool (ICAT). ICAT emphasizes legal and regulatory ramifications, training and inspection programmes, programme assessment and auditing, monitoring of food-borne illness and outbreaks, compliance, community relations, programme resources, international communication and laboratory support. SRAs inherently work both ways as partner agencies evaluate the FDA under similar guidelines that must be consistently met for renewal every five years. This system naturally creates a common framework for food safety and communication and is a demonstration of international cooperation to create a reciprocal agreement anchored in common objectives.

APEC Cross-Border Privacy Rules (CBPR) System[21]

This is an initiative of the Asia-Pacific Economic Cooperation (APEC), which includes the US, Japan, Canada and other countries. CBPR promotes regulatory reciprocity by ensuring that member-countries adhere to a common set of privacy principles when handling personal data.

US-Israel MoU on Cybersecurity[22]

The US and Israel finalized an MoU on cybersecurity cooperation that includes the mutual recognition and acceptance of cybersecurity regulations to ensure the security of critical infrastructure and information systems.

EU-Japan agreement[23]

Japan has regulatory reciprocity with the EU, wherein the European Commission has recognized Japan's data protection laws as equivalent to its own, allowing data to flow freely between these regions.

> **The SCRE community supports regulatory reciprocity between regions and countries to increase interoperability and security, and to reduce costs.**

Conclusion

Cybersecurity in the electricity sector has grown ever more important. Multiple concurrent trends are amplifying the risk landscape: the proliferation of digitized and interconnected devices within energy infrastructure, a surge in attacks targeting this infrastructure, a transformation in the sector due to the energy transition, which challenges established regulatory assumptions, and the emergence of powerful capabilities in both defence and offense through technologies such as artificial intelligence.

Across the globe, regulators, including those in the United States, often employ diverse approaches to address similar cybersecurity challenges due to the absence of a universal consensus on cybersecurity standards. Consequently, this leads to complex and generalized regulations across various industries and sectors, resulting in a fragmented, inconsistent and sometimes conflicting regulations. This impedes interoperability. Further, as the cybersecurity threat landscape evolves, regulatory bodies respond by introducing additional regulations, exacerbating the issue by increasing costs, introducing inefficiencies, and impacting the cybersecurity posture of both sectors and organizations. The diversion of limited resources away from addressing cybersecurity challenges also carries opportunity costs.

The World Economic Forum's Systems of Cyber Resilience: Electricity Initiative community has identified global regulatory interoperability as a primary focus area by establishing the Global Regulations Working Group. Its mission is to facilitate interoperability of global cyber regulations in the electricity sector. The working group is working towards creating common community positions among its members to help regulators and government agencies that function as regulators better understand the needs of the sector.

This white paper presents the community's response to the request for information issued by the White House Office of the National Cyber Director (ONCD) of the US on 19 July 2023. It specifically answers questions in the international section (Section 9) that focuses on addressing conflicts in cybersecurity requirements, identifying priority sectors and regions, evaluating international dialogues, reviewing ongoing global initiatives, and exploring regulatory reciprocity.

The community's recommendations for the ONCD are as follows:

1. Continue ONCD's ongoing efforts to increase global regulatory interoperability, improve security and lower costs.

2. Prioritize security over compliance by adopting a risk-based approach to regulation.

3. Engage private, public and civil society stakeholders from the earliest stage of the policy and regulatory process.

4. Leverage existing international technical standards issued by non-government bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

5. Participate in international dialogues and international initiatives on cybersecurity.

Contributors

Lead Author

Kesang Tashi Ukyab
Lead, Cyber Resilience, Electricity,
World Economic Forum

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity,
World Economic Forum

SCRE Global Regulations Working Group Leads

Christophe Blassiau
Senior Vice-President, Cybersecurity and Product Security; Global Chief Information Security Officer and Chief Product Security Officer, Schneider Electric, France

Yuri G. Rassega
Chief Information Security Officer (CISO) Head of Cyber Security, Enel, Italy

SCRE community

Jose Manuel Alonso Barril
Chief Information Security Officer (CISO),
Iberdrola, Spain

Stefano Bracco
Knowledge Manager, Agency for the Cooperation of Energy Regulators, Slovenia

Manny Cancel
SVP and CEO of E-ISAC, NERC, USA

Tim Conway
Director of SCADA and ICS, SANS Institute, USA

Sebastijan Cutura
Policy Manager, European Cyber Security Organisation (ECSO), Belgium

Todd Davies
Head of Cyber Risk Quantification & Strategy Trends, Vestas, Denmark

Mark Antony D'Ambrogio
Regional Information Security Officer, Orsted, United Kingdom

Gabriele De Luca
Cybersecurity Program Manager, Enel, Italy

Joe Doetzl
Global Chief Information Security Officer (CISO),
Hitachi Energy, USA

Morten Duus
Chief Information Security Officer (CISO), Vestas, Denmark

Mikhail Falkovich
Chief Information Security Officer (CISO),
Consolidated Edison, USA

Peter Frøkjær
Senior Security Architect, Vestas, Denmark

Loris Gasparrini
Head of Cyber Security Standards and External Stakeholders, Enel, Italy

Agustín Valencia Gil-Ortega
OT Security Business Development, Fortinet, Spain

David Andres Hurtado
Head of OT Cybersecurity & Resilience, Naturgy, Spain

Frederik Lilleøre Jæger
Chief Information Security Officer, Orsted, Denmark

Rosa Kariger
Global Security Governance & Intelligence,
Iberdrola, Spain

Jesus Sanchez Lopez
Head of Global Cybersecurity, Naturgy, Spain

Stuart Madnick
John Norris Maguire Professor of Information Technologies and Professor of Engineering Systems, MIT – Sloan School of Management, USA

Angelica Marotta
Affiliated Researcher, Cybersecurity, Massachusetts Institute of Technology, USA

Paulo Moniz
Director - Information Security and IT Risk, EDP - Energias de Portugal, Portugal

Charmaine Ng
Director, Digital Policy, Asia-Pacific, Schneider Electric, Singapore

Goran Novkovic
Head of Critical Infrastructure Protection, NEOM, Saudi Arabia

Ranjan Pal
Research Scientist, Massachusetts Institute of Technology, USA

Trevor Rudolph
Vice President, Global Digital Policy & Regulation, Schneider Electric, USA

Gabriella Serino
Cyber Security Standards & External Stakeholders Specialist, Enel, Italy

Leo Simonovich
Vice President and Global Head, Industrial Cyber and Digital Security, Siemens Energy, USA

Henrik Loth Thiesen
Vice President, Cyber Strategy & Commercialization, Enterprise Cyber Security, Vestas, Denmark

Philip Tonkin
Chief of Staff, Dragos, United Kingdom

Maximilian Urban
Information Security Officer and Innovation Manager, Netz Niederösterreich, Austria

Swantje Westpfahl
CEO, Institute for Security and Safety (ISS), Germany

Tom Wilson
SVP & Chief Information Security Officer (CISO), Southern Company, USA

Sander Zeijlemaker
Research Affiliate, Cybersecurity, Massachusetts Institute of Technology, USA

The Forum also wishes to acknowledge contributions from **John La Rue**, Consultant at La Rue Writing LLC.

Annex 1: Related publications

1. Matter standard for interoperability of smart homes and internet of things devices
   https://csa-iot.org/wp-content/uploads/2023/02/Consumer-IoT-Device-Cybersecurity-Standards-Policies-and-Certification-Schemes.pdf

2. US-Japan Cyber Dialogue
   https://www.mofa.go.jp/press/release/press4e_003253.html

3. France-UK Cyber Dialogue
   https://www.gov.uk/government/news/uk-france-cyber-dialogue-11-may-2023

4. European Union Agency for Cybersecurity (ENISA)
   https://www.enisa.europa.eu/

5. The Internet Engineering Task Force (IETF)
   https://www.ietf.org/

6. The APEC Cross-Border Privacy Rules (CBPR) System
   https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system

7. US-Israel Memorandum of Understanding (MoU) on Cybersecurity
   https://home.treasury.gov/news/press-releases/jy0929

8. EU-Japan Agreement
   https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4501

9. Cyber Resilience in the Electricity Ecosystems: Principles and Guidance for Boards
   https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

10. Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors
    https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf

11. Cyber Resilience in the Electricity Ecosystems: Playbook for Boards and Cybersecurity Officers
    https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Playbook_for_Boards_and_Cybersecurity_Officers_2020.pdf

12. Cyber Resilience in the Electricity Ecosystems: Securing the Value Chain
    https://www3.weforum.org/docs/WEF_Securing_the_Electricity_Value_Chain_2020.pdf

13. European Commission's Cybersecurity Package: Commentary in light of recent sophisticated supply chain attacks
    https://www3.weforum.org/docs/WEF_Commentary_in_light_of_recent_sophisticated_supply_chain_attacks_2021.pdf

14. IEA Cybersecurity – is the power system lagging behind?
    https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

15. A SANS 2021 Survey: OT/ICS Cybersecurity
    https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

16. White House National Cybersecurity Strategy
    https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Endnotes

1. Executive Office of the President of the US, "Request for Information on Cyber Regulatory Harmonization", https://www.whitehouse.gov/wp-content/uploads/2023/07/ONCD-Reg-Harm-RFI-Final-July-19.2023.pdf.
2. The White House, "National Cybersecurity Strategy", https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
3. World Economic Forum, "Strengthening the cybersecurity of the power grid", https://www.weforum.org/impact/cybersecurity-in-electricity/.
4. CSA Singapore, "Cybersecurity Labelling Scheme (CLS)", https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.
5. Council of the European Union, "The European Cyber Resilience Act (CRA)", https://www.european-cyber-resilience-act.com/.
6. Federal Communications Commission, "Certificate Mark – U.S. Cybersecurity Labeling Program for Smart Devices", https://www.fcc.gov/cybersecurity-certification-mark.
7. IEA, "Cybersecurity – is the power system lagging behind?" https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind.
8. SANS, "A SANS 2021 Survey: OT/ICS Cybersecurity", https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/.
9. US Department of State, "The 2022 U.S.-EU Cyber Dialogue", https://www.state.gov/the-2022-u-s-eu-cyber-dialogue/.
10. Ministry of Foreign Affairs of Japan, "The 8th Japan-US Cyber Dialogue", https://www.mofa.go.jp/press/release/press4e_003253.html.
11. Gov.uk, "UK-France Cyber Dialogue", https://www.gov.uk/government/news/uk-france-cyber-dialogue-11-may-2023.
12. ISO, "ISO/IEC AWI 27404", https://www.iso.org/standard/80138.html.
13. ETSI, "ETSI EN 303 645", https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.
14. NIST, "NIST IR 8425", https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf.
15. ENISA, https://www.enisa.europa.eu/.
16. Internet Engineering Task Force (IETF), https://www.ietf.org/about/introduction/.
17. Connectivity Standards Alliance (CSA), https://csa-iot.org/.
18. OMDIA, "Matter standard", https://csa-iot.org/wp-content/uploads/2023/02/Consumer-IoT-Device-Cybersecurity-Standards-Policies-and-Certification-Schemes.pdf.
19. European Commission, "Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows", https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.
20. US Food and Drug Administration, "Systems Recognition", https://www.fda.gov/food/international-cooperation-food-safety/systems-recognition-food.
21. APEC, "What is the Cross-Border Privacy Rules System", https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.
22. US Department of the Treasury, "Treasury Announces Cyber Security Cooperation Memorandum of Understanding (MoU) with the State of Israel", https://home.treasury.gov/news/press-releases/jy0929.
23. European Commission, "The European Union and Japan agreed to create the world's largest area of safe data flows", https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4501.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org