The Software Alliance

BSA

BSA INTERNATIONAL CYBERSECURITY POLICY FRAMEWORK

CONTENTS

INTRODUCTION

Governments around the world confront an increasingly complex and diverse array of cybersecurity threats. Each year, cyber crime drains hundreds of billions of dollars from the global economy, disrupting business services, inhibiting innovation, and stifling job growth. Malicious hackers, including state-sponsored actors, threaten critical infrastructure and government services, risking widespread economic damage and even loss of life. Unfortunately, these risks are no longer hypothetical: around the world, malicious cyber activity has created power outages, closed ports, disrupted financial transactions, and interfered with national elections.

The ability of governments to effectively confront these threats depends on crafting smart, agile policies to support a balanced, comprehensive approach to cybersecurity. By adopting the right mix of laws and rules and creating the appropriate institutions and structures that establish clear guidance on cybersecurity, governments can create a sound foundation for defending against malicious cyber actors, taking full advantage of the opportunities of the digital economy, and enhancing cooperation with stakeholders. These steps will help all parties involved, from national governments to private-sector actors, in the joint effort that is needed to effectively protect systems and prevent, mitigate, and respond to cyber attacks.

Yet, because cybersecurity threats remain relatively new and are evolving so quickly, governments are often in a position of playing catch-up, with little guidance on best practices or model policies. To support governments as they consider the most effective policy approaches to defending against cybersecurity threats, BSA | The Software Alliance offers this comprehensive cybersecurity policy framework as a model for consideration by policymakers as they assess their current cybersecurity policies and seek to identify priority areas for improvement.

BSA's International Cybersecurity Policy Framework provides a recommended model for a comprehensive national cybersecurity policy. It is intended to serve as a tool both for policymakers considering foundational cybersecurity legislation and for those examining gaps and shortfalls in existing policies. BSA views strong and smart cybersecurity policy as a critical ingredient to the stability of the Internet and the vibrancy of the global economy. For that reason, BSA will evaluate the proposed policies of governments around the world against the principles articulated by this Framework.

The Framework is divided into three sections. First, a quick-reference summary identifies key elements of the model framework. Second, each element is examined in-depth, offering specific principles for crafting policy approaches in each area. Finally, the Framework proposes definitions for commonly used terminology. Throughout the document are highlighted international examples of best practices in implementing cybersecurity policies.

As cybersecurity threats grow more sophisticated and more dangerous, the risks of insufficient or poorly calibrated national policy approaches to countering cyber threats are growing increasingly catastrophic. BSA looks forward to partnering with governments around the world to increase security and resilience of the increasingly interconnected Internet ecosystem for the billions of global citizens that rely upon it. As the cybersecurity threat landscape evolves, BSA will continually assess governments' progress and adjust this framework to help policymakers keep pace.

SECTION I. EXECUTIVE SUMMARY

BSA recommends that policymakers seek to root all cybersecurity policies in six overarching principles:

1. **Policies Should Be Aligned with Internationally Recognized Technical Standards.** Internationally recognized technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cybersecurity, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability.

2. **Policies Should Be Risk-Based, Outcome-Focused, and Technology-Neutral.** Malicious cybersecurity activity carries different risks for different systems. There are generally multiple approaches to defending against the same type of cyber attack, and multiple approaches to improving system security and resiliency in general. Policies should reflect these variables, prioritizing approaches that address different levels of risk and enable owners and operators of networks and systems to defend their infrastructure with the technologies and approaches they deem best to meet the level of security desired.

3. **Policies Should Rely on Market-Driven Mechanisms Where Possible.** Information technology is constantly evolving, and cybersecurity threats evolve with it. Neither technologies nor threats are bound by national borders, meaning that overreliance on government structures or regulatory enforcement is unlikely to achieve desired results. Policies that leverage market forces to drive cybersecurity are likely to be most successful in keeping pace with the changing security environment and in achieving the broadest effect.

4. **Policies Should Be Flexible and Adaptable to Encourage Innovation.** Information technology and the millions of jobs technology supports depend on the ability to innovate new solutions. Cybersecurity requires constant innovation to keep pace with changing threats. Policies must be flexible and adaptable to enable businesses to develop new approaches to new challenges, and to deliver innovative products to the customers that depend on them.

5. **Policies Should Be Rooted in Public-Private Collaboration.** Cybersecurity is a shared responsibility across government and private stakeholders. Although governments often hold critical cybersecurity tools and information, the private sector is responsible for significant elements of the critical infrastructure and the technology platforms that are targeted by malicious cyber activity, as well as many of the cybersecurity tools and services necessary to defend against such threats. Only by working in close collaboration with the private sector can governments truly combat cybersecurity threats while sustaining the vitality of the digital economy.

BSA'S GUIDING PRINCIPLES FOR CYBERSECURITY POLICY

Cybersecurity policies should adopt approaches that are:

1 Aligned with **internationally recognized standards**

2 **Risk-based, outcome-focused, technology-neutral**

3 **Market-driven** where possible

4 **Flexible and adaptable** to encourage innovation

5 Rooted in **public-private collaboration**

6 Oriented to **protect privacy**

6 **Policies Should Be Oriented to Protect Privacy.** No approach to cybersecurity should compromise the integrity of the data it seeks to defend against malicious cyber activity; cybersecurity policies should be carefully attuned to privacy considerations. Key considerations include ensuring civilian leadership, encouraging strong data protections, protecting personal information in information-sharing mechanisms, and avoiding policies that undermine the use of privacy-enhancing technologies.

Rooted in these principles, BSA's International Cybersecurity Policy Framework outlines a comprehensive foundation for cybersecurity policy, including detailed principles to guide legislative and administrative action. The following chart summarizes the key elements of a strong national cybersecurity policy.

KEY ELEMENTS OF A NATIONAL CYBERSECURITY POLICY

GOVERNMENT ORGANIZATION AND STRATEGY

Structure	☑	Establish a Single National Body Responsible for Cybersecurity
	☑	Clearly Define Stakeholder Roles and Responsibilities
	☑	Establish a Functional, Timely Interagency Process
Strategy and Plans	☑	Issue a National Cybersecurity Strategy
	☑	Issue a Critical Infrastructure Cybersecurity Strategy
	☑	Maintain Up-to-Date National Cybersecurity Incident Response Plan for Critical Infrastructure
	☑	Craft Sector-Specific Plans as Appropriate
Stakeholder Engagement	☑	Establish Structure for Facilitating Public-Private Partnerships
	☑	Create Mechanism for Supporting National and Sub-National Governments

CYBERSECURITY AND THE GOVERNMENT

Preparedness and Response	☑	Establish and Resource National Computer Emergency Response Team
	☑	Authorize and Encourage Timely Threat Information-Sharing
	☑	Ensure Calibrated Structure for Incident Reporting
	☑	Ensure a Consistent, Reasonable Standard for Personal Data Breach Notification
	☑	Establish a Transparent, Coordinated Process for Government Handling and Disclosure of Vulnerabilities
Government Procurement	☑	Keep Acquisition Technology Neutral
	☑	Ensure Use of Licensed Software
	☑	Ensure Software Is Vendor-Backed
	☑	Leverage the Security Benefits of Cloud Services
	☑	Build Security Considerations into Acquisition Processes
	☑	Manage IT Systems Smartly and Securely
	☒	Avoid Domestic Preference Requirements
Research and Development	☑	Support Research and Development of Cybersecurity Technologies and Tools

CYBERSECURITY AND THE PRIVATE SECTOR

Critical Infrastructure	☑	Focus on Security Outcomes
	☑	Use Risk-Based, Flexible Policy Framework
	☒	Avoid Overbroad Definition of Critical (Information) Infrastructure
	☑	Align Critical Infrastructure Security with Internationally Recognized Standards
	☒	Avoid Indigenous Security Standards
	☑	Ensure Any Certification Regimes Are Balanced, Transparent, and Internationally Based
	☒	Reject Requirements to Disclose Source Code and Other Intellectual Property

KEY ELEMENTS OF A NATIONAL CYBERSECURITY POLICY

CYBERSECURITY AND THE PRIVATE SECTOR *(continued)*		
Consumer Products	☑	Promote Market-Driven Solutions
	☑	Ensure Any Certification Schemes Are Voluntary, Market-Driven, Broad-Based, and Internationally Aligned
	☑	Encourage Adoption of Internationally Recognized Standards
Data Flows	☑	Enable Cross-Border Data Flows for Business Purposes
	☒	Avoid Data Localization Requirements
	☑	Maintain a Policy Environment That Enables Emerging Technologies
CYBERSECURITY AND THE CITIZEN		
Awareness	☑	Invest in Public Cybersecurity Awareness
	☑	Create Tools to Inform Consumer Choices
Workforce Development	☑	Build Cybersecurity Awareness into Every Level of Education
	☑	Prioritize Diversity in Cybersecurity Education and Training
	☑	Support Alternative Pathways to Cybersecurity Careers
CRIMINAL CODES		
Cyber Crime	☑	Establish a Comprehensive Legal Framework Consistent with Budapest Convention on Cyber Crime
	☑	Apply Criminal Liability Only to Actors with Criminal Intent
	☑	Provide Technical Training and Support for Law Enforcement
INTERNATIONAL ENGAGEMENT		
Fostering International Cybersecurity Cooperation	☑	Integrate Cybersecurity Cooperation into Foreign Policy
	☑	Engage in International Cooperative Efforts
	☒	Ensure Export Control Policies Do Not Impede Legitimate Cybersecurity Activity
Upholding International Obligations	☑	Prevent Territory from Being Used for International Cyber Attacks
	☑	Protect Privacy and Human Rights on the Internet
	☒	Avoid Mandates That IT Systems Manufacturers Support State-Sponsored Hacking

SECTION II. IN DEPTH

BEST PRACTICE

National Competent Authority for International Network and Information Security Coordination

Effective collaboration depends on clear, open lines of communication and agile coordination across a range of stakeholders. To facilitate such collaboration, a best practice is identifying a National Competent Authority (NCA) for network and information security, as directed in the European Union's 2016 Network and Information Security Directive. The NCA serves as the "single point of contact" to liaise with other governments in support of cross-border cooperation against transnational cybersecurity threats, and promote sharing of critical cybersecurity information across national stakeholders. The single national body assigned lead responsibility for cybersecurity will often serve as the NCA.

Government Organization and Strategy

Structure

Establish a Single National Body Responsible for Cybersecurity. While responsibilities for key policies and activities relating to cybersecurity may be distributed across numerous government agencies, identifying a single government body with lead responsibility for the government's cybersecurity can ensure clarity, coherence, and coordination in the government's preparedness for and response to cybersecurity threats and challenges. Governments should identify a single organization with lead responsibility for cybersecurity and empower that organization to direct and oversee the cybersecurity efforts of other government agencies. In general, because of the broad ramifications for national and international economic interests, overall cybersecurity efforts should be led by a civilian entity (see Section III, Definitions).

Clearly Define Stakeholder Roles and Responsibilities. Each nation organizes and governs itself differently, and cybersecurity responsibilities can be effectively assigned and distributed in many different ways. Some nations prefer centralized models, with cybersecurity policy efforts limited to a narrow group of government agencies, whereas others prefer models in which responsibilities are more widely distributed across the government. Whichever model is chosen, it is critical that roles and responsibilities for all relevant stakeholders—including cabinet offices, government agencies, industry stakeholders, and non-government organizations—be clearly defined and assigned in such a way as to avoid confusion or redundancy.

Establish a Functional, Timely Interagency Process. Regardless of how a government organizes itself for cybersecurity, cybersecurity policies will affect the activities and objectives of multiple government agencies, including both civilian and military agencies. A functional interagency process is essential to balancing interests across these agencies and adjudicating disputes when they arise. Moreover, an interagency structure must establish processes to achieve resolution to time-sensitive decisions in a timely manner.

Strategy and Plans

Issue a National Cybersecurity Strategy. A national cybersecurity strategy sets out a nation's overall approach to cybersecurity, and is a critical document for ensuring national-level strategic and policy coherence. An effective national cybersecurity strategy will outline the cybersecurity threat faced by the nation, identify and prioritize objectives, delineate roles and responsibilities among key government and industry stakeholders, and establish timeframes and metrics for implementation. Furthermore, it will situate national cybersecurity activities in the context both of international cybersecurity activities and of other national activities that affect cybersecurity efforts. A national strategy is important not only for guiding government initiatives, but also for raising awareness of key issues among decision-makers and informing the public about government policies and activities. Such a strategy should be developed cooperatively through consultation with representatives of all relevant stakeholders, including government agencies, industry, academia, and citizens groups. It should be issued at the national level, ideally by the head of government, and should integrate central, sub-national, and local government approaches, as well as community-based best practices within a national context. Finally, it should include specific taskings, deadlines, and metrics to ensure it is effectively implemented.

Issue a Critical Infrastructure Cybersecurity Strategy. Governments also should assess and establish clear priorities among the critical services and infrastructures (see Section III, Definitions) that most need protection. For example, electricity grids, water supply systems, and transportation systems serve to meet basic human needs, and generally are prioritized for protection under national critical infrastructure strategies. Within sectors, however, not all assets, systems, networks, data, and services are equally essential; it is important that the strategy avoid overreaching and imposing compliance burdens where they are not necessary. Treating non-critical systems in the same way as those that are truly critical will not only unnecessarily slow the pace of innovation and growth but also risk misallocating limited security resources. Accordingly, it is important that decision makers assess the national infrastructure, based on objective criteria and the input of relevant stakeholders, and determine those that are providing critical services and functions, and whose compromise, damage, or destruction through a significant cybersecurity incident (see Section III, Definitions) could result in significant harm to the public. As a government assesses and prioritizes critical infrastructures for protection, its results should feed into a critical infrastructure protection plan. Such a plan identifies priority critical infrastructures and outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

Maintain Up-to-Date National Cybersecurity Incident Response Plan for Critical Infrastructure. Although a critical infrastructure protection plan defines how government agencies and other stakeholders in a nation's critical infrastructure community will manage risk and defend against threats, a national incident response plan defines how these stakeholders will respond to a significant cybersecurity incident (see Section III, Definitions). Informed by international best practices, such a plan should articulate the roles and responsibilities, capabilities, and coordinating structures that support how a nation will respond to and recover from significant cybersecurity incidents affecting critical infrastructure. A national incident response plan provides guidance to enable a unified whole-of-government, whole-of-nation, and internationally coordinated approach to response and recovery during a significant cybersecurity incident affecting critical infrastructure. It articulates common doctrine and a strategic framework for national, sector, and individual organization cyber operational plans.

BEST PRACTICE

Convene Multi-Stakeholder Processes

The government can play an important role by convening targeted working groups, focused on a specific challenge or threat, that maximize the capabilities of the most relevant public and private sector stakeholders. Although private industry stakeholders are often willing to collaborate to address prominent current cybersecurity threats, such cooperation can be accelerated when a government is able to identify and convene relevant stakeholders, leveraging both its convening power and its intelligence-informed understanding of challenges and threats. Multi-stakeholder processes ensure that inputs from all relevant stakeholders in both government and private sector roles are addressed in the formation of a policy or operational initiative, and that stakeholders are invested in the outcomes.

Craft Sector-Specific Plans as Appropriate. Although certain elements of cybersecurity protection apply across all areas, and many recommendations are available from national and international organizations, there also is a need for guidance that is tailored to the business needs of particular entities or that provides methods to address unique risks or specific operations in certain sectors.

Stakeholder Engagement

Establish Structure for Facilitating Public-Private Partnerships. Effective cybersecurity requires collaboration and coordination among all stakeholders. Real partnership between public and private sectors is particularly important because non-government entities manage and operate many critical infrastructures, often including those that control transportation, health, banking, energy, and other vital sectors. Governments should establish laws and structures to facilitate public-private partnerships on a voluntary basis. At minimum, such laws and structures should address: (1) structure, legal authority, and protections for voluntary sharing of threat and vulnerability information; (2) legal authority for voluntary public-private operational collaboration to disrupt cybersecurity threats; (3) mechanisms for awareness and outreach activities; and (4) intra-sector public-private collaboration.

Create Mechanism for Supporting Sub-National and Local Governments. Government functions at the sub-national and local level can often be as or even more important in supporting the daily lives and activities of citizens and businesses as are those at the national level, yet sub-national and local governments generally cannot maintain the same level of capability in defending against cyber attacks that may disrupt these functions as would the national government. Sub-national and local governments are themselves critical infrastructures, and national policies should establish mechanisms for defending them, including by providing technical and/or financial assistance to sub-national and local governments to develop their own robust cyber defenses.

Cybersecurity and the Government

Preparedness and Response

Establish and Resource National Computer Emergency Response Team. Incident-response capabilities should be established to manage the most critical and significant events that threaten the confidentiality, integrity, or availability of nationally significant information networks and systems, or that create widespread risk to individual citizens. Computer emergency response teams (CERTs) at the national and sub-national or local levels, as well as computer security incident response teams (CSIRTs), can play a crucial role in improving cyber resilience. These entities can (1) provide incident response services to victims of attacks; (2) share information concerning vulnerabilities and threats with key stakeholders in the government, private sector, and, in some instances, the broader public; and (3) offer other ways of helping improve computer and network security. National governments should legally establish computer emergency response teams at the national level, and ensure sufficient resourcing to such teams to capably prepare for and address significant cybersecurity incidents and other large-scale national cyber events.

Authorize and Encourage Timely Threat Information-Sharing. The ability to share information about cybersecurity threats, vulnerabilities, and incidents with affected parties as well as entities with capabilities to develop means to defend against attacks is indispensable. Because attacks are aimed at both private sector and government actors, and across national borders, information sharing policies should promote sharing between the government and the private sector, among private sector entities, and between government entities. To that end, effective cybersecurity information sharing laws or policies should be crafted according to six tenets:

1. **Safe Harbor from Liability.** Policies should empower private entities to voluntarily share information regarding cybersecurity threat indicators (see Section III, Definitions) with other private entities or with governments, domestically and internationally, by expressly limiting potential legal liability or regulatory consequences. This limitation should apply for both sharing and receiving this information. Moreover, consistent with the voluntary basis of such an approach, policies should ensure that companies are not held liable for choosing not to share information with other private entities or governments.

2. **Privacy.** Policies should protect the privacy of those affected by shared cybersecurity threat information without impeding the ability to share cybersecurity threat indicators in a timely fashion.

3. **Multi-Directional Sharing.** Policies should facilitate information sharing by private entities with both government and private parties, and from the government to private parties, while providing flexibility to affected parties to enter into appropriate transactional and sector-specific arrangements.

4. **Timeliness.** Policies should authorize and encourage government actors to share relevant cybersecurity threat information with private parties, and accelerate the time periods for sharing such information, including through automated mechanisms.

5. **Civilian-Led.** Policies should establish a civilian portal for private-to-government information sharing.

6. **Cybersecurity Use.** Policies should ensure shared cybersecurity threat information is used by the recipient only to promote cybersecurity and for no other purpose, and when information is shared with governments, that the information is used only to promote cybersecurity or for limited law enforcement activities.

Ensure Calibrated Structure for Incident Reporting. Some governments have sought to improve their situational awareness of and response to the cybersecurity threat landscape by adopting measures to either encourage voluntary reporting, or require mandatory reporting, to government or regulatory entities of significant cybersecurity incidents (see Section III, Definitions). Voluntary incident reporting regimes can strengthen trust between government and industry and facilitate more robust two-way information-sharing; it is important such regimes, whether mandatory or voluntary, be targeted in a risk-based manner. Frameworks with overbroad thresholds for reporting can unintentionally inhibit cybersecurity by causing companies to over-notify for any incident on their systems, leading to notification fatigue, increased costs, operational distractions, and difficulties identifying and addressing the most important incidents. Instead, governments seeking to establish a mechanism for cyber incident reporting should adopt the following principles:

» **Establish a Clear Reporting Structure.** Given that numerous government and regulatory agencies could be involved in a particular incident, an efficient, accessible reporting structure should be put in place, ideally coordinated through a national computer emergency response team. This structure must be supported with technical capabilities ensuring safe and agile transmission and use of the data.

- Calibrate Reporting Threshold According to Risk. Not every cyber incident is important, and over-reporting can overwhelm entities on the receiving end, leaving them less responsive to significant threats. Instead, reporting should be limited to (1) critical infrastructure sectors most important to the nation; (2) incidents that substantially affect the confidentiality, availability, or integrity of the affected system; and (3) actionable information regarding the incident.
- Avoid Duplicative Requirements. Incident reporting policies should define roles and responsibilities, including those of both government actors and reporting entities, so as to avoid duplication of reporting requirements, even when reporting entities are accountable to multiple regulatory regimes. Governments should prevent duplicative requirements across individual government agencies, seeking to streamline processes for sharing information about significant incidents in order to promote effective and efficient responses.
- Maintain Consistency. Different reporting requirements for different industries or different situations drive confusion and contribute to undue regulatory burdens. Instead, incident reporting frameworks should be flexible, practical in the business environment, based on internationally recognized standards and other widely accepted approaches, and consistent across sectors.
- Avoid Mandatory Timelines. Artificially short timelines generate incomplete or inaccurate reporting, and often require affected entities to report information before they have a full picture or diagnosis of the incident. Incident reporting frameworks should create an expectation that incidents are reported in a reasonable timeframe without compromising the integrity of reporting or mandating specific deadlines.

Ensure a Consistent, Reasonable Standard for Personal Data Breach Notification. Creation of a breach notification system for personal data applicable to all businesses and organizations can provide incentives for entities to ensure robust protection for personal data, while enabling data subjects to act to protect themselves in the event their data is compromised. Any such system, however, must be carefully crafted to prevent the issuance of immaterial notices. Notice should only be required where there is a serious risk of harm to the user. Notice should not be required where the lost data in question has been rendered unusable, unreadable, or indecipherable to an unauthorized third party through practices or methods, which are widely accepted as effective industry practices or industry standards at the time of the breach. If a breach notification is required, it should occur in a reasonable timeframe, considering the time required to evaluate the nature and scope of the breach and whether the breach is likely to cause significant harm to data subjects. Artificially short timelines can undermine completeness and accuracy of reporting, and interfere with incident response. Instead, notification standards should create an expectation that incidents are reported in a reasonable timeframe without compromising the integrity of reporting or mandating specific deadlines.

Establish a Transparent, Coordinated Process for Government Handling and Disclosure of Vulnerabilities. Governments should establish clear, principle-based policies for handling product and service vulnerabilities that reflect a strong mandate to report them to vendors in line with Coordinated Vulnerability Disclosure principles[1] rather than to stockpile, buy, sell, or exploit them. Coordinated Vulnerability Disclosure programs reduce the potential for damage by ensuring vendors can fix vulnerabilities before they are made public, incentivize responsible approaches to security research and vulnerability disclosure, and help both governments and technology vendors avoid surprises. Such policies should be transparent to the public.

[1] See, for example, ISO/IEC 29147 (Vulnerability Disclosure), available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip or *The CERT Guide to Coordinated Vulnerability Disclosure*, available at https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

Government Procurement

Keep Acquisition Technology Neutral. Effective cybersecurity involves layered, multi-faceted approaches to defending networks; as such, innovative cybersecurity solutions can leverage many technical approaches to achieve common objectives. To ensure government agencies are able to obtain the most innovative, effective cybersecurity solutions, acquisition rules and regulations should be technology neutral. Procurement policies should specify security objectives, but leave the technical approaches regarding how to best meet those objectives to vendors to decide.

Ensure Use of Licensed Software. The use of unlicensed software exposes enterprises and government agencies to heightened risks of malware infections and other security vulnerabilities. In fact, a 2015 study by global research firm IDC identified a strong correlation between the presence of unlicensed software and the incidence of malware encounters.[2] Because unlicensed software is less likely to receive critical security updates that would otherwise mitigate the risks associated with malware exposure, its use heightens the risk of harmful cybersecurity incidents. Unlicensed technology from untrusted sources may also contain embedded malware inserted by malicious actors. Unfortunately, the use of software that is not properly licensed, including by government agencies and contractors, is still a significant problem globally. In many cases, the use of unlicensed software by governments may be simply a function of government agencies lacking awareness of the software assets resident on their systems. Most agencies do not have adequate policies for managing software licenses. Transparent and verifiable software asset management (SAM) practices identify situations where entities are using unlicensed software, as well as situations where the licenses they have far exceed the number of users. Under-licensing creates legal liability and security risks, while over-licensing creates inefficiencies and unnecessary costs. Government agencies should adopt SAM practices based on internationally recognized standards for their own procurement and software asset management, improving cybersecurity and reducing costs by ensuring that they only use properly licensed software. Furthermore, government agencies should require their component offices, as well as contractors supporting them, to adopt robust software asset management practices.

Ensure Software Is Vendor-Backed. As government agencies increasingly purchase and "consume" IT resources as online services, rather than as products, it becomes more imperative than ever that government agencies work with IT suppliers with a proven track record of offering robust and reliable support for their offerings. Government policies should therefore encourage government agencies to place a premium on selecting IT solutions for which the supplier (or some other commercial partner) offers reliable support, and should ensure that vendors are compensated for ongoing product support and updates, as appropriate. This recommendation should apply equally to all IT solutions, regardless of licensing or development model. Commercial systems, hardened by ongoing testing and proven in the marketplace, may often prove more reliable and secure than untested custom-built approaches. Open-source technology can be integrated into government IT systems but, unless backed by vendor support to manage ongoing security patches and upgrades, such systems can introduce risk into government networks.

Leverage the Security Benefits of Cloud Services. Cloud computing services are the backbone of the modern economy, empowering innovative business and government solutions and generating unprecedented connectivity, productivity, and competitiveness. In addition, cloud services often provide security benefits that can help governments improve their posture against cybersecurity threats. To leverage these benefits, governments should adopt policies that encourage migration to cloud services and ensure that procurement policies are modernized to enable cloud services to compete on a level playing field. Traditional purchasing practices and contract terms may hinder the scalable, cost-effective, and innovative nature of cloud computing. Quick and flexible procurement processes that are not hampered by burdensome terms and conditions will allow users to fully leverage the vast array of benefits offered by cloud computing technologies.

[2] John L. Gantz et al., "Unlicensed Software and Cybersecurity Threats," *International Data Corporation White Paper* (January 2015), available at http://globalstudy.bsa.org/2013/Malware/study_malware_en.pdf.

Build Security Considerations into Acquisition Processes. Many countries adopt regulations guiding acquisition of products for the government, including rules intended to ensure the government gets maximum value for its investments. In some cases, this legitimate intent has translated into mandates that products offering the lowest price should be preferred, regardless of other circumstances. Such rules, in the context of information technology procurements, often discourage government agencies from selecting products or services that offer the greatest value to the agency. That additional value can manifest itself in many different ways—for instance, in the form of better security, additional functionality, superior product support, or greater ease of use. These rules may also restrict an agency's consideration of past performance as a factor in the procurement process, thus forcing it to ignore information that may, as a practical matter, be highly relevant. Such rules create a substantial risk that government agencies are forced to select the "cheapest" solution, even if that solution does not provide the lowest overall cost of ownership and does not offer the best value for the government's money. Instead, governments should adopt "best value" contracting policies, in which proposals are assessed according to cost, value, past performance, security, and other variables to ensure that governments maximize the return on their investments.

Manage IT Systems Smartly and Securely. Ensuring cybersecurity in government IT systems extends beyond smart purchasing decisions; it requires smart management of systems throughout their life cycles. The changing threat landscape requires continual development of cybersecurity technologies, smart management, sustained planning, and adequate budgeting around IT systems with a focus on cybersecurity; specifically, policies governing government agency IT acquisitions should:

- **Keep Software and Systems Up-to-Date.** Many significant data breaches take advantage of outdated or unpatched software and systems; government agencies should plan and budget to maintain up-to-date software and systems.
- **Plan for Ongoing Security.** Too often, well-intentioned government agencies seek to implement custom software solutions to fix specific problems without plans for ensuring and sustaining security of those solutions. Government agencies should establish plans for ongoing security, including updating/patching, of software and IT systems before those solutions are integrated, and such plans should be maintained throughout the product life cycle. Governments should also lead the transformation of skills and job profiles required to meet future security demands by investing in cybersecurity capabilities of developers, engineers, and related work profiles.
- **Incorporate SAM.** Transparent and verifiable software asset management (SAM) practices, based on international recognized standards, help government agencies secure IT inventories by identifying uses of unlicensed software, which often remains unpatched and vulnerable, and taking action to remediate it.

Avoid Domestic Preference Requirements. Cutting-edge products and services are developed through global collaboration in research and design centers across many different countries. Countries should create incentives for cross-border collaboration to facilitate rapid and innovative solutions to shared security challenges, including through government acquisition policies. However, some countries take the opposite approach, assuming that by preventing foreign competition they can protect domestic champions, develop an indigenous technology industry, and defend against perceived cybersecurity risks of foreign products. Indigenous technologies represent only a subset of global innovation. Preventing foreign competition in government procurements reduces cybersecurity by denying government agencies access to world-class products and services. Furthermore, such policies deprive domestic technology firms of valuable opportunities to collaborate with global leaders and make them less competitive internationally, harming global innovation. Opening procurements to solutions from the global marketplace will increase efficiency, cut costs, and improve security.

Research and Development

Support Research and Development of Cybersecurity Technologies and Tools. Investing in research and development (R&D) provides a concrete means for governments to advance cybersecurity. Such R&D can help governments foster technological solutions to identified gaps and challenges, as well as to develop new approaches to building security into broader government systems. R&D investments help to support a domestic cybersecurity ecosystem in industry and academia. Moreover, R&D can be targeted beyond individual technologies to develop tools for improving cybersecurity; such tools can range from examining new applications of existing technologies to supporting the development of internationally recognized standards and best practice frameworks to guide organizational approaches to specific cybersecurity challenges.

Cybersecurity and the Private Sector

Critical Infrastructure

Fundamental to a country's cybersecurity policy is a framework for ensuring cybersecurity across critical infrastructure. Because in most countries critical infrastructure operators largely reside in the private sector, it is important that such a framework promotes close public-private collaboration and reflects the needs and objectives of all stakeholders.

Focus on Security Outcomes. Critical infrastructure sectors are often diverse in terms of technological infrastructure, involve different types of risk, and confront different threats and threat actors. Moreover, the technologies used in these infrastructures are diverse and constantly evolving. Overly directive regulation focusing on specific methods or strict compliance, or mandates that limit the use of security-enhancing technologies such as encryption, rather than improving security, can bog down adaptive security measures and stifle innovation of new security technologies. Instead, governments should focus critical infrastructure cybersecurity policies on driving desired security outcomes, providing private sector entities latitude to develop the most effective, innovative approaches to meet those security outcomes. Outcome-based approaches that integrate risk assessment tools, maturity models, and risk management processes enable organizations to prioritize cybersecurity activities and make informed decisions about cybersecurity resource allocation to align defenses against the most pressing risks.

Use Risk-Based, Flexible Policy Framework. Technology evolves rapidly and in unpredictable new directions; it is thus essential that any policy framework for critical infrastructure cybersecurity undertake security measures that are sufficiently adaptable to avoid stifling innovation and economic development. To achieve this balance, a critical infrastructure cybersecurity framework should be based on the following key principles:

1. **Risk-Based and Prioritized.** Cybersecurity threats come in many forms and magnitudes with varying degrees of severity. Establishing a hierarchy of priorities—based on an objective assessment of risk (see Section III, Definitions)—with critical assets and/or critical sectors at the top is an effective starting point from which to ensure that cyber protections are focused on those areas where the potential for harm is greatest.

2. **Technology-Neutral.** A technology-neutral approach to cybersecurity protection is vital to ensure access to the most secure and effective solutions in the marketplace. Specific requirements or policies that mandate or prohibit the use of certain technology only undermine security by restricting evolving security controls (see Section III, Definitions) and best practices and potentially creating single points of failure.

3. **Practicable.** Overly burdensome government supervision of private operators or disproportionately intrusive regulatory intervention in their operational management of cybersecurity risk most often proves counterproductive, diverting resources from effective and scalable protection to fragmented administrative compliance. Instead, a framework should establish standards and security measures that are accessible and scalable across the range of covered entities.

BEST PRACTICE

NIST Framework for Improving Critical Infrastructure Cybersecurity

The United States National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is a voluntary, risk-based approach to managing cybersecurity risk that is intended to be applicable and scalable for organizations of all sizes and types, including critical infrastructure operators. It is structured around five core functions that reflect the full life cycle of cybersecurity risk management: identify, protect, detect, respond, and recover. These functions are further subdivided into 22 categories and 98 subcategories of guidance, which are mapped to internationally recognized standards (such as the ISO/IEC 27000 family of information security management systems standards) and other informative references. As such, the Framework:

- ✓ Is risk-based, flexible, and outcome-oriented
- ✓ Aligns with internationally recognized standards and risk management approaches
- ✓ Embraces public-private partnership
- ✓ Avoids dependency on indigenous technical standards
- ✓ Avoids burdensome regulatory schemes

The Framework is the baseline cybersecurity policy approach to strengthening cybersecurity across critical infrastructure. In fact, the United States Government has directed that all federal government agencies, including the Defense Department and the Intelligence Community, use the Framework to guide their risk management programs. The Framework, according to available data, has been widely adopted by critical infrastructure operators, and it is expected that it will be adopted by more than 50 percent of all US organizations by 2020. Several other nations have begun to adopt substantively similar framework approaches, such as Italy's National Cyber Security Framework and Malaysia's MDEC Cybersecurity Industry Development Framework.

4. **Flexible.** Managing cyber risk is a cross-disciplinary function and no one-size-fits-all approach exists. Each industry, system, and business faces distinct challenges, and the range of responsible actors must have flexibility to address their unique needs.

5. **Respectful of Privacy and Due Process.** Security requirements should be duly balanced with the need for protection of privacy and due process. Ensuring that requirements and obligations are proportionate, do not represent more intrusion in privacy rights than what is strictly necessary, follow due process, and are supported by adequate judicial oversight are all important considerations to address in any critical infrastructure cybersecurity framework.

Avoid Overbroad Definition of Critical (Information) Infrastructure. Broad definitions cause uncertainty among business owners, their providers, and government agencies for compliance and during enforcement. Such definitions are likely to create costly regulatory burdens without actually improving cybersecurity, overwhelming infrastructure operators with obligations best reserved for those involved in supporting truly essential systems. Overly broad definitions can also lead to overwhelming regulatory authorities with unnecessary information and oversight/enforcement responsibilities. Instead, governments should adopt a definition of critical (information) infrastructure (see Section III, Definitions) that focuses on truly essential systems, and apply a rigorous, proportionate, and risk-based analysis to determine what specifically should be designated critical (information) infrastructure.

Align Critical Infrastructure Security with Internationally Recognized Standards. Standards and best practices are most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. Regulations, policies, and standards issued by a government to address critical infrastructure cybersecurity should be aligned with internationally recognized technical standards (see Section III, Definitions) and internationally recognized approaches to risk management, such as the ISO/IEC 27000 and ISO/IEC 62443 series of information security (see Section III, Definitions) management standards, the Common Criteria for Information Technology Security Evaluation, or the NIST Framework for Improving Critical Infrastructure Cybersecurity, as appropriate. Governments should particularly emphasize alignment with those standards developed through voluntary, consensus-based processes. Allowing critical infrastructure operators to combat evolving cybersecurity threats with evolving best practices and standards permits a more flexible, current, and risk-based approach to cybersecurity. Moreover, use of internationally recognized standards ensures interoperability for both businesses and government agencies with international counterparts, facilitating both economic development and operational collaboration against cybersecurity threats.

Avoid Indigenous Security Standards. Some governments are imposing country-specific standards for critical infrastructure cybersecurity, arguing that market-specific rules will lead to improved cybersecurity. The real effect, however, is the opposite. Government-imposed indigenous standards inconsistent with globally accepted best practices and standards, rather than bolstering security, tend to freeze innovation and force consumers and businesses into using products that might not suit their needs. Such an approach can prevent critical infrastructures from integrating security technologies that represent best-in-class solutions.

Ensure Any Certification Regimes Are Balanced, Transparent, and Internationally Based. Certification regimes (see Section III, Definitions) may be effective measures to drive stronger cybersecurity in the critical infrastructure community, but they must be structured in a way that both promotes security needs and addresses market demands for both continuing innovation and broad diversity of product types and configurations. Therefore, any certification regime should be based on internationally recognized standards or risk management approaches (for example, the ISO/IEC 27000 and ISO/IEC 62443 series of information security management standards or the NIST Framework for Improving Critical Infrastructure Cybersecurity, both of which are widely used to manage risk and improve cybersecurity for critical infrastructure operators globally). These international approaches feature the ongoing, iterative development of standards and risk management practices that allow certification frameworks to maintain currency as technology develops, and incorporate input and best practices from government and private sector stakeholders on a global basis. Certification regimes should emphasize software security-by-design principles by including process-based standards for software development that incorporate security considerations throughout the development process, such as the ISO/IEC 27034 series of standards. These process-based approaches recognize the importance of integrating security from inception, but also account for the agile and iterative nature of modern software development. Moreover, certification regimes used in the critical infrastructure sector should be (1) transparent, ensuring that businesses operating critical infrastructure or providing products or services to

BEST
PRACTICE

Ensure Any Certification Schemes Are Voluntary, Market-Driven, Broad-Based, and Internationally Aligned

Product certification or labeling schemes may be effective measures to improve consumer awareness and drive stronger product cybersecurity, but they must be structured in a way that reflects market demands for both continuing innovation and broad diversity of product types and configurations. Therefore, certification and labeling schemes should be strictly focused on voluntary, consensus-based, and industry-led initiatives, including self-assessment schemes, that are linked to proven internationally recognized standards. Moreover, relying upon a voluntary, consensus-based, and industry-led standard setting process cannot be an effective approach unless the approach is adopted on a wide scale. Market-driven incentives for adopting any certification or labeling standards are preferable to other alternatives. Requiring adoption through legislation or using adoption to shape insurance markets and legal liability may have the unintended result of impeding flexible, outcome-oriented standards and eroding innovation. Instead, governments should craft market-driven incentives for participation in certification schemes.

critical infrastructure operators are provided with full visibility into certification standards, methodologies, processes, and outcomes; and (2) independent, allowing for use of internationally accredited certification bodies rather than requiring exclusive use of specific in-country entities.

Reject Requirements to Disclose Source Code and Other Intellectual Property. Some countries have begun to impose laws requiring developers of certain products to make source code and related intellectual property available for inspection before such products can be used in critical infrastructure. Such requirements are inappropriate and ineffectual. Requirements to disclose source code, enterprise standards, security testing results, and similar proprietary information pose significant inherent risks to intellectual property protection, while providing little added security value. Because many of today's technology products include hundreds of thousands or even millions of lines of code, inspectors simply are not capable of reliably identifying single code flaws. If governments store code disclosed by software developers, it can be targeted by hackers for theft, and can then potentially be used by an attacker discover and refine attack methods. Governments should avoid any law requiring the transfer of, or access to, source code of as a condition for the import, distribution, sale or use of such software, or of products containing such software.

Consumer Products

Promote Market-Driven Solutions. With technologies, security approaches, and consumer demands constantly changing, heavy-handed regulatory approaches cannot keep pace with the dynamism and diversity of the market. Instead, the most effective means of promoting cybersecurity in consumer markets will be to harness the power of the market to drive greater security. Market-driven solutions come in a range of forms, including industry-led internationally recognized standards development and adoption, industry consortiums, tax incentives, safe harbors, and voluntary certification and labeling schemes. When crafting policy frameworks to tackle consumer product cybersecurity, governments should adopt such market-driven solutions, tailored to their own distinct circumstances, and avoid mandatory regulatory measures.

Encourage Adoption of Internationally Recognized Standards. Technology standards (see Section III, Definitions) play a vital role in enabling and enhancing cybersecurity. By supporting internationally recognized technical standards that are developed with industry participation and accepted across markets, companies can more quickly develop, distribute, and adopt newer and more secure products. Moreover, using internationally recognized standards ensures interoperability for both businesses and government agencies with international counterparts, facilitating both economic development and operational collaboration against cybersecurity threats. Therefore, governments should ensure that any regulations, laws, or policies regarding cybersecurity in consumer products should be aligned with internationally recognized technical standards and internationally recognized approaches to risk management.

Data Flows

Enable Cross-Border Data Flows for Business Purposes. The modern economy depends upon cloud computing services and other technologies that allow the storage, processing, and transfer of data across multiple locations and across international borders. By allowing data to flow freely among multiple markets, these technologies drive international trade, cross-border business collaboration, economies of scale, and increasingly, technological solutions to common governance challenges such as pandemic disease and disaster response. Moreover, these technologies bring security benefits such as reliability, resiliency, and 24-hour security support. Laws that restrict the cross-border transfer of data for business purposes undermine both economic and security benefits, and should be avoided in national cybersecurity legal and policy frameworks.

» **Promote Privacy, Security, and Cross-Border Data Flows.** Some countries' cybersecurity regimes have established restrictions on cross-border data flows with an objective of securing data, either for privacy or security purposes, or both. Yet, such restrictions are unnecessary, and often counterproductive, for achieving effective data security. While an enforceable international consensus on cross-border data rules does not exist, responsible data stewardship should be based on internationally recognized principles of transparency and accountability, as articulated in the Organisation for Economic Co-operation and Development (OECD) "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" and embodied, for example, by the Asia Pacific Economic Cooperation (APEC) Privacy Framework.

» **Distinguish between Data Processors and Data Controllers.** In any personal data protection regime, it is important to distinguish between data controllers and data processors in order to provide clarity on the responsibilities and liabilities vis-à-vis the data subject or owner, and also for facilitating compliance with legal requirements. The data controller should be the entity responsible for compliance with obligations relating to personal data. Data processors only act on behalf of data controllers. Data processors treat data based on a mandate given by the data controller so the data processor's obligations should be mostly governed by contracts with clear limits to liability for data processors under the measures.

Avoid Data Localization Requirements. Based on the mistaken assumption that data is safer in a specific location, some countries are imposing rules that require data to be stored domestically. In fact, data localization requirements not only impede global commerce by undermining the benefits of cloud computing services and other technologies that underpin the modern economy; they also forgo many security benefits that such technologies can bring, such as redundancy, around-the-clock security monitoring, cloud-based network defense tools, and others. Data localization requirements are among the most counterproductive approaches to cybersecurity, and should be avoided in nearly all circumstances.

Maintain a Policy Environment That Enables Emerging Technologies. Emerging technologies are increasingly important cybersecurity tools. Artificial intelligence (AI)-enabled cyber tools, for instance, are used to help analysts parse through hundreds of thousands of security incidents per day to weed out false positives and identify threats that warrant further attention by network administrators. Because cybersecurity threats come from around the world, the data used to train AI-enabled cyber tools needs to be able to move across borders. Policies that inhibit data transfers or that limit the ability to analyze traffic data to identify threats will also impede the use of emerging technologies for cybersecurity.

Cybersecurity and the Citizen

Awareness

Invest in Public Cybersecurity Awareness. The vast majority of cyber breaches and attacks are attributable to poor individual cyber hygiene. Governments that invest in increasing public awareness of the shared role of governments and citizens in protecting computers and networks can drive society-wide cybersecurity and cyber resilience. There are many ways governments can invest in public awareness; successful efforts have included national awareness events (such as dedicating a national cybersecurity awareness week or month), public service advertising campaigns, dedicated websites and online guidance, social media campaigns, and school events. Another important way the government can promote cybersecurity awareness is by making available aggregate and publicly disclosed data about cybersecurity incidents to enable researchers, policymakers, and average citizens better understand the scope and contours of cybersecurity challenges.

Create Tools to Inform Consumer Choices. A critical—and often ignored—element of improving cybersecurity is promoting the adoption of secure products and security services by both individual and enterprise consumers. Too often, consumers lack the ability to make informed decisions that differentiate between products based on security, or to understand the comparative value of security products or services. Governments can help improve cybersecurity by emphasizing cybersecurity awareness and developing tools to enable consumers to obtain and compare critical product security information in the marketplace, empowering them to contribute to enhancing cybersecurity across the information technology ecosystem.

Workforce Development

Build Cybersecurity Awareness into Every Level of Education. Building a cybersecurity workforce to meet current and future needs begins with educating a broader generation of future practitioners. Governments should invest in programs to ensure that cybersecurity education at every level of the education system is available, accessible, and aligned both to the needs of the cybersecurity workforce and to emerging cybersecurity challenges. Governments should consider programs to (1) expose young people to cybersecurity concepts, including basic cyber hygiene, through primary school curricula; (2) increase interest in and access to cybersecurity education among youth through scholarships and research competitions; and (3) incentivize the development, accreditation, and promotion of cybersecurity-focused education programs through universities, community colleges, and other educational venues.

Prioritize Diversity in Cybersecurity Education and Training. Around the world, women and ethnic minorities tend to be significantly underrepresented in the cybersecurity workforce, representing a damaging inability to leverage the talents and perspectives of huge segments of the labor pool. As governments invest in wider efforts to provide education to future cybersecurity professionals, they should leverage such programs to incentivize more female and minority students to pursue cybersecurity education. Moreover, government investments should aim to make cybersecurity education and career opportunities available broadly, beyond urban capitals and industrial centers. As the cybersecurity jobs gap—the gap between available positions and qualified individuals available to fill them—continues to grow, there are vibrant communities of talented young female and minority students, from both urban and rural areas,who can help meet the demand, provided governments adopt smart policies to engage and attract them to this vital field.

Support Alternative Pathways to Cybersecurity Careers. Cybersecurity expertise can be developed through alternative pathways that do not require university or graduate degrees, including through apprenticeship programs, community colleges, cybersecurity "boot camps" or short-term intensive training academies, and relevant government or military service. Governments should invest in fostering these alternative pathways. In addition, although investing in educating young people to fill the cybersecurity jobs of tomorrow is critical, the growth of digital commerce is proceeding at a pace that requires an influx of new cybersecurity professionals in the near-term. Investing in re-training opportunities to enable mid-career professionals to transition into cybersecurity careers can help bridge the cybersecurity workforce shortfall in the near-term, while also helping communities evolve to support the changing workforce demands of the 21st-century economy.

Criminal Codes

Cyber Crime

Establish a Comprehensive Legal Framework Consistent with Budapest Convention on Cyber Crime. Nations should establish comprehensive legislation addressing criminal liability, investigations, and prosecutions in the cyber domain. Such legislation should be crafted in accordance with the Budapest Convention on Cybercrime,[3] which serves a guideline for developing comprehensive national legislation against cyber crime (see Section III, Definitions) and as a framework for international cooperation between State Parties to this treaty. The Convention includes requirements for substantive laws (minimum standards for what is criminalized); procedural mechanisms (investigative methods); and international legal assistance (such as cross-border access to digital evidence or extradition). The legal framework should provide support for cross-border investigations.

Apply Criminal Liability Only to Actors with Criminal Intent. Malicious actors often carry out cyber crimes by taking advantage of vulnerabilities in privately owned cyber assets, ranging from individual computers to major networks. Among the more significant cybersecurity threats, for example, are botnets, which commandeer thousands of individual computers and direct them to take actions to degrade another system or network. When cyber vulnerabilities in privately owned assets are exploited by malicious actors as part of a cyber attack (see Section III, Definitions), owners of such assets are victims of the attack just as are the attack's targets; the criminal offender is the malicious cyber actor who exploits such vulnerabilities. Criminal prosecution should be reserved for those seeking to disrupt, degrade, or destabilize cyberspace, and not those who are the victims of such malicious activity. Moreover, criminal codes should distinguish between the illegitimate activities of malicious actors and the legitimate research and testing of security professionals designed to strengthen cybersecurity, who may use related tools and techniques.

Provide Technical Training and Support for Law Enforcement. As digital technologies continue to evolve, law enforcement organizations around the world must continue to adapt investigative techniques to technological innovations, particularly in order to be able to investigate and prosecute cyber crimes effectively. Governments should consider mechanisms to provide adequate technical training and technical support, potentially including the establishment of specialized cyber units, to ensure that law enforcement organizations maintain sufficient investigative capabilities as technology changes. Governments should avoid policies that mandate technical specifications to enable law enforcement access, as such technical specifications can weaken cybersecurity.

International Engagement

Fostering International Cybersecurity Cooperation

Integrate Cybersecurity Cooperation into Foreign Policy. Cybersecurity is a transnational challenge that demands international cooperative solutions; such cooperation depends upon effective, proactive diplomacy. Governments should express a commitment to international cooperation on cybersecurity and recognize it as a key priority for their foreign policy. In strategy documents, organization, and budgets, governments should emphasize strong, collaborative cybersecurity as a critical element of national security

[3] The Convention on Cybercrime of the Council of Europe (CETS No. 185), entered into force January 7, 2004, available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.

and should develop and articulate clear areas of focus to promote cooperation. These areas of focus might include participating in multi-national operational collaboration to confront specific cybersecurity threats, supporting the establishment of international cybersecurity norms or confidence building measures, building the cybersecurity capacity of foreign partners, participating in international cybersecurity standards development, or participating in multilateral governance mechanisms. Establishing a lead cybersecurity diplomat may help some governments focus and synchronize diplomatic efforts across these areas.

Engage in International Cooperative Efforts. International cybersecurity cooperation is taking root in two important areas: multilateral governance efforts and operational collaboration. Multilateral governance enables national governments to develop common policies and standards that serve as a shared foundation to enhance security and deepen economic linkages. International fora and cooperation mechanisms, including international policy and standards bodies, centers of excellence, regional and global events, intergovernmental discussions, public and private alliances, and other collaboration mechanisms help nations develop common rules of the road, protocols for cooperation and incident response, shared standards, and common infrastructure to enable operational collaboration. Operational collaboration—real-time, practical cooperation to address specific incidents or threats, such as collaboration on law enforcement investigations or response to cybersecurity incidents with transnational effect—helps national governments receive timely information on potential threats and vulnerabilities and be able to respond quickly to any incidents as a result. Governments should participate in both types of collaboration to ensure that their needs and priorities are addressed within the context of these multilateral frameworks, and to uphold the shared responsibility of defending global networks against malicious cyber activity.

Ensure Export Control Policies Do Not Impede Legitimate Cybersecurity Activity. Securing critical networks and infrastructure against malicious intrusions, exploits, vulnerabilities, and other emerging cybersecurity threats requires real-time testing and remediation efforts. To combat the rapidly evolving threat landscape, cybersecurity professionals must be able to freely share information about emerging threats and solutions with large communities of experts around the world. Network defenders require access to technologies that share many of the technical attributes of the very threats they are attempting to defend against. For instance, cybersecurity professionals make use of "penetration testing" tools to evaluate whether a network is vulnerable to known and emerging software exploits and hacking techniques. To effectively mitigate those network vulnerabilities, companies must be able to share information about vulnerabilities and exploits freely and in real time. Export controls that inhibit the real-time sharing of the vulnerabilities and exploits that the penetration testing tools rely on would severely affect the ability to create safe products and ensure a secure network and IT environment. Efforts to regulate the spread of malicious software through use of export controls must therefore be narrowly tailored so that they do not inadvertently impose restrictions on cybersecurity professionals, incident responders, or the independent research community.

Upholding International Obligations

Prevent Territory from Being Used for International Cyber Attacks. Beyond defending their own systems and networks against cyber attacks, governments have a responsibility to prevent malicious cyber actors from using their territory to launch or support cyber attacks against other nations. Legal frameworks criminalizing malicious cyber activity should cover such activity even when victims are beyond a nation's borders. Moreover, sufficient enforcement mechanisms should be put in place to identify and disrupt those involved in international cyber attacks.

Protect Privacy and Human Rights on the Internet. Governments should pass laws to implement UN resolutions protecting human rights and privacy on the Internet, including laws to promote access to the Internet, protect the right to expression on the Internet, protect privacy in digital communications, and ensure adequate legal remedies are available to individuals whose privacy or human rights have been violated. Furthermore, governments should avoid policies that undermine the development and use of privacy-enhancing technologies.

Avoid Mandates That IT Systems Manufacturers Support State-Sponsored Hacking. Although espionage and other state-sponsored cyber activities are conducted by many governments, attempts by governments to force technology providers to support or be complicit in such activities can create tremendous negative consequences for international commerce. As such, governments should avoid any laws that serve as mandates for technology providers to support state-sponsored cyber activities, including mandating government access features (often called "backdoors"), requiring disclosure of encryption keys or source code, requiring cooperation with intelligence agencies, or requiring surveillance of citizens outside the context of lawfully authorized surveillance of criminal suspects.

SECTION III. DEFINITIONS

Certification. Certification may be defined as "third-party attestation (i.e., issue of a statement) that specified requirements related to products, processes, systems or persons have been fulfilled."

Civilian Entity. A civilian entity may be defined as "a government organization or government-sponsored organization that does not have primary responsibility for law enforcement, intelligence collection or analysis, defense, or the armed forces."

Computer System. Consistent with the Budapest Convention on Cybercrime, a computer system may be defined as "any device or a group of interconnected or related devices, on or more of which, pursuant to a program, performs automatic processing of data."

Computer Data. Consistent with the Budapest Convention on Cybercrime, computer data can be defined as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."

Continuous Monitoring. Continuous monitoring may be defined as "the ongoing or near real-time process used to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time in light of changing information technology and threat development."

Countermeasure. A countermeasure may be defined as "an automated or manual action or actions to modify, redirect, or block information known or suspected to contain cybersecurity threat indicators that is stored on, processed by, or transiting an information system that is for the purpose of protecting an information system from cybersecurity threats. A countermeasure is a defensive measure conducted on an information system:

- Owned or operated by the party to be protected;
- Operated on behalf of the party to be protected; or
- Operated by a private entity providing electronic communication services, remote computing services, or cybersecurity services to the party to be protected."

Critical Information Infrastructure. As with critical infrastructure, the definition of critical information infrastructure may require modification based on the context and intent of its use. In general, critical information infrastructure can be defined as follows:

> "Critical information infrastructure refers to information and communications technology systems that are themselves critical infrastructures or that are essential for the operation of critical infrastructures, such that their destruction, degradation, or unavailability would have a large-scale, debilitating impact on national security, public health, public safety, national economic security, or core government functions."

Critical Infrastructure. Definitions for critical infrastructure may need to be more broad or more narrow, depending on the context in which the term is being used. Moreover, beyond a legal definition of the term, a national government should maintain risk-based processes for identifying specific critical infrastructure assets, services, and systems.

However, in general, critical infrastructure can be defined as follows:

> "Critical infrastructure refers to those assets, services, and systems, whether physical or virtual, which, if destroyed, degraded, or rendered unavailable for an extended period, would have a large-scale, debilitating impact on national security, public health, public safety, national economic security, or core state or federal government functions. Specific critical infrastructures are identified based on analysis of criticality, interdependency, and risk."

Cyber Attack. A cyber attack can be defined as "an action intended to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system."

Cyber Crime. Consistent with the Budapest Convention on Cybercrime, cyber crime may be defined as follows:

> "criminal offenses against the confidentiality, integrity, and availability of data and systems or unauthorized access to systems, to include the following actions, when committed intentionally:
>
> 1. Illegal access: the access to the whole or any part of a computer system without right.
> 2. Illegal interception: the interception without right, made by technical means, or non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.
> 3. Data interference: the damaging, deletion, deterioration, alteration, or suppression of or denial of access to computer data without right.
> 4. System interference: the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.
> 5. Misuse of devices: the production, sale, procurement for use, import, distribution or otherwise making available of (a) a device, including a computer program or computer code, designed or adapted primarily for the purpose of committing any of the offenses listed above, or (b) a computer password, access code, credential, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offenses listed above."

Cybersecurity Incident. A cybersecurity incident may be defined as "a single, or series of, identified occurrence(s) of a system, service, or network indicating a possible breach of information security policy or failure of security controls, or a previously unknown situation that may be relevant to the security of the system, service, or network."

Cybersecurity Services. Cybersecurity services may be defined as "products, goods, or services, that are primarily designed to detect, mitigate, or prevent cybersecurity threats."

Cybersecurity Threat. A cybersecurity threat may be defined as "any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system."

Cybersecurity Threat Indicator. A cybersecurity threat indicator may be defined as follows:

> "information that is necessary to describe or identify:
>
> 1. Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
> 2. A method of defeating a security control or exploitation of a security vulnerability;
> 3. A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
> 4. A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the

defeat of a security control or exploitation of a security vulnerability;

5. Malicious cyber command and control;
6. The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
7. Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
8. Any combination thereof."

Defensive Measure. A defensive measure may be defined as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."

Information Security. Information security may be defined as follows:

> "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide:
>
> 1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity;
> 2. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
> 3. Availability, which means ensuring timely and reliable access to and use of information."

Information System. An information system may be defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

Internationally Recognized Standard. A standard may be defined as "a document, established by international consensus, approved by a recognized body, and widely adopted that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Standards are voluntary agreements, developed within an open process that gives all international stakeholders, including consumers, the opportunity to express their views and have those views considered. This contributes to their fairness and market relevance, and promotes confidence in their use."

Risk. Risk can be defined as "an expression of the effect of uncertainty on cybersecurity objectives, as understood through the analysis of identified threats to a product or system, the known vulnerabilities of that product or system, and the potential consequences of the compromise of the product or system."

Security Control. A security control may be defined as "a management, operational, or technical control used to protect against unauthorized efforts to adversely affect the confidentiality, integrity, and availability of an information system or its information."

Significant Cybersecurity Incident. A significant cybersecurity incident may be defined as "a cybersecurity incident resulting in:

- The unauthorized or denial of access to or damage, deletion, alteration, or suppression of data that is essential to the operation of critical infrastructure; or
- The defeat of an operational control or technical control that is essential to the security or operation of critical infrastructure."

ABOUT BSA

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

The Software Alliance

BSA

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

☎ +1.202.872.5500
@BSAnews
@BSATheSoftwareAlliance

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

☎ +65.6292.2072
@BSAnewsAPAC

BSA Europe, Middle East & Africa

65 Petty France
Ground Floor
London, SW1H 9EU
United Kingdom

☎ +44.207.340.6080
@BSAnewsEU