1 November 2019

**Cyber Security Policy Division**
**DEPARTMENT OF HOME AFFAIRS**
By online submission

**AUSTRALIA'S 2020 CYBER SECURITY STRATEGY – BSA COMMENTS**

BSA | The Software Alliance is grateful for this opportunity to make a submission on the Australian government's 2020 Cyber Security Strategy (**2020 Strategy**), and the issues raised in the discussion paper released by the Australian government in connection with its call for views on this important matter[1] (**Discussion Paper**).

## A. Statement of Interest

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[2] are at the forefront of data-driven innovation that is fuelling global economic growth by helping enterprises in every sector of the economy operate more efficiently. BSA's members earn users' confidence by providing essential security technologies to protect against cyber threats posed by a broad range of malicious actors, including those who would harm citizens and their loved ones, steal identities and commercially valuable secrets, or pose an immediate danger to national security.

BSA members have made significant investments in Australia and are proud that many Australian organisations and consumers continue to rely on BSA member products and services to support Australia's economy. BSA and our members thus have a significant interest in the Australian government's 2020 Strategy.

## B. Introduction

The world is more connected now than ever with half the world's population now online. The growth of the internet, the proliferation of connected devices, and the explosion in cloud-enabled processing capabilities have given rise to new opportunities that have the potential to improve almost every

[1] As published on: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020.

[2] BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

aspect of our lives. Indeed, as a recent report[3] observes, technology is a critical component of modern economies like Australia, with the technology sector contributing 6.6% of Australian GDP, employing over half a million workers, supporting many small and medium-sized businesses, and underpinning innovation and productivity growth in almost every other industry.

With these opportunities, however, there also come risks, including large-scale data theft, privacy violations, phishing scams, ransomware, and malicious information operations that affect millions of people around the world each year.

Addressing this challenge requires innovative cybersecurity practices and tools to defend the integrity, privacy, and utility of the Internet ecosystem, and we offer the comments and recommendations below in the hope that these will be useful to aid the Australian government in considering how best to position Australia to "meet cyber threats, now and into the future"[4] with the 2020 Strategy.

Our submission focuses on:

a. guiding principles and elements for the 2020 Strategy; and

b. three specific questions in the Discussion Paper, concerning the existing regulatory environment, 'built in' security for digital goods, and services and instilling better trust in ICT supply chains.

## C. Guiding Principles and Elements for the 2020 Strategy

As a general response to the various questions posed in the Discussion Paper concerning the roles, functions, and responsibilities of the government, the industry, and consumers, BSA **recommends that** the Australian government should consider rooting the 2020 Strategy, and all future cyber security policies adopted thereunder, in six overarching guiding principles, which have been derived from BSA's and BSA's members' experience working on cyber security issues with government around the world:

1. Policies should be aligned with internationally recognised technical standards. Internationally recognised technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cyber security, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. Alignment with internationally recognised technical standards and guidance, as such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Technical Report 27103, can ensure that Australia benefits from proven approaches to cyber defence and is even better-positioned to cooperate inter-operably with the international community in confronting transnational threats, especially with respect to essential services systems[5] protection.

   Interoperability is a particular concern in areas – such as security of Internet of Things technologies and cloud computing services – where gaps in internationally recognised technical standards have sparked the proliferation of different government- and industry-

[3] AlphaBeta, *Australia's Digital Opportunity: Growing a $122 Billion a Year Tech Industry*, September 2019, available at: https://www.alphabeta.com/our-research/australias-digital-opportunity-growing-a-122-billion-a-year-tech-industry/

[4] As noted on page 5 of the Discussion Paper.

[5] Which the Discussion Paper notes at page 15, and at various other portions, is at high risk of malicious activity.

driven approaches. BSA strongly urges the Australian government to embrace multilateral, interoperable initiatives to address security in these areas rather than to seek to develop national standards that could duplicate and potentially conflict with existing efforts. Where there are gaps in internationally recognised technical standards, BSA calls upon the Australian government to work with other government and industry partners to address those gaps, building a basis for policies that can improve security consistently and cooperatively across different markets.

2. Policies should be risk-based, outcome-focused, and technology-neutral. Malicious cyber security 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. The 2020 Strategy should prioritise approaches and policies 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 cyber security 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 incentivise and leverage market forces to drive cyber security are likely to be the most successful in keeping pace with the changing security environment and in achieving the broadest effect.

4. Policies should be oriented to protect privacy. No approach to cyber security should compromise the integrity of the data it seeks to defend against malicious cyber activity; cyber security 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. Australia has already taken a commendable principles-based, outcomes-focused approach to privacy and personal information protection, primarily through the Australian Privacy Principles. The 2020 Strategy should continue to embrace the enabling effect that this principles-based approach has had on innovation and development of the digital economy in Australia.

5. 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. Likewise, cyber security 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. In this respect, we commend the Australian government for already recognising the need for flexible laws in the Discussion Paper.[6]

6. Policies should be rooted in public-private collaboration. Cyber security is a shared responsibility across government and private stakeholders. Although governments often hold critical cyber security 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 cyber security tools and services necessary to defend against such threats. Only by working in close collaboration with the private sector can

[6] At page 11 of the Discussion Paper.

governments truly combat cyber security threats while sustaining the vitality of the digital economy. In this respect, we are pleased to note that the Discussion Paper already calls out the need for the 2020 Strategy to be developed and supported through partnership and collaboration with the industry.[7]

Aligned with the six guiding principles above, BSA **further recommends that** the Australian government should consider incorporating into the 2020 Strategy the following elements, which are described in further detail in the *BSA International Cybersecurity Policy Framework*[8] (attached as **Annex A** to this submission), and which have again been developed through BSA's and BSA's members' experience working on cyber security issues globally:

1. Relating to the government: government organisational structures, cyber security strategy and plans (including for critical infrastructure), stakeholder engagement mechanisms, preparedness and response processes, procurement policies, support for research and development, and international engagement and co-operation.[9]

2. Relating to the private sector: outcomes-focused and risk-based policies for critical information infrastructure cyber security, market-driven solutions for consumer products, and support for cross-border data flows and enablement of emerging technologies.[10]

3. Relating to citizens and the workforce: public cyber security awareness initiatives and tools, and programs and support for cyber security education, training, and career development.[11]

4. Relating to cyber-crime: a comprehensive legal framework consistent with the *Budapest Convention on Cyber Crime*[12] and law enforcement technical training and support to address cyber-crime.[13]

## D. Specific Questions in the Discussion Paper

In this section, we focus on three specific questions posed in the Discussion Paper:

- Question 10: "*Is the regulatory environment for cyber security appropriate? Why or why not?"*
- Question 12: "*What needs to be done so that cyber security is 'built in' to digital goods and services?*"
- Question 13: "*How could we approach instilling better trust in ICT supply chains?*"

[7] At pages 5 and 15 of the Discussion Paper.

[8] Available at: http://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework/.

[9] As described on pages 6-13 and 19-21 of BSA's *International Cybersecurity Policy Framework.*

[10] As described on pages 13-18 of BSA's *International Cybersecurity Policy Framework.*

[11] As described on pages 18-19 of BSA's *International Cybersecurity Policy Framework.*

[12] The *Convention on Cybercrime of the Council of Europe* (CETS No. 185), available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[13] As described on pages 19-20 of BSA's *International Cybersecurity Policy Framework.*

### Question 10*: "Is the regulatory environment for cybers security appropriate? Why or why not?"*

In general, BSA believes the Australian government has created a regulatory environment that promotes strong cyber security without constraining innovation or digital commerce. However, the government's adoption of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (**Assistance and Access Act**) has created concerns about Australia's ability and commitment to embrace the most effective cyber security policies and technologies.

Strong encryption represents a critically important cyber security technology. It underpins data security, identity management, and protection of devices against unauthorised access. It also plays a crucial role in defending critical infrastructure systems. Yet, notwithstanding limitations on mandating the weakening of encryption within the legislation, the Australian government has framed the *Assistance and Access Act* as an authority necessary to enable Australian law enforcement and intelligence officials to gain access to encrypted data and devices. Security experts around the world have recognised that any conceivable approach to ensuring law enforcement access to encrypted data will result in a weakening of the encryption technology in use.

As the Australian government considers and develops the 2020 Strategy, it must pursue policies that address both the threats of today and the threats of tomorrow. Promoting strong and ubiquitous encryption is essential both now and into the future. As Australia embraces 5G technology, for example, encryption – and end-to-end encryption, particularly – will take on even greater importance as a way to protect massive volumes of data traversing increasingly decentralised, potentially untrusted network infrastructure. Likewise, encryption has also been identified as key to securing the Internet of Things.

To position the Australian government to embrace technologies that will best protect Australia from malicious cyber-attacks, BSA **recommends that** the Australian government should revisit the *Assistance and Access Act* and work with the industry to communicate, in implementing guidance and public messaging, that encryption should remain inviolable and to promote the adoption of strong encryption wherever appropriate and necessary.

### Question 12*: "What needs to be done so that cyber security is 'built in' to digital goods and services?"*

BSA commends the Australian government for recognising that there is a need for digital products and services to have security built in "by-design". Given that malicious actors increasingly target vulnerabilities in software to attack critical networks and systems, software security has emerged as an urgent priority. Software developers, their customers, and policymakers need tools to describe, assess, and encourage security across the entire software lifecycle, from its development to the end of its life.

As the Australian government has noted, however, "visible and trusted industry standards do not yet exist in most cases".[14] Indeed, there has not been a holistic framework that articulates best practices for software security in a way that can be specifically described and effectively measured across diverse development environments, software types, and coding languages.

[14] At page 13 of the Discussion Paper.

To fill this significant gap in international cyber security policy, BSA has developed the *BSA Framework for Secure Software*[15] (**Secure Software Framework**)(attached as **Annex B** to this submission). Building on best practices pioneered by many of BSA's members, the Secure Software Framework tackles complex security challenges through an adaptable and outcome-focused approach that is risk-based, cost-effective, and repeatable. It is intended to encourage security-by-design in software products and services, as well as in the myriad products that depend upon software (from consumer Internet of Things devices to Industrial Control Systems), by helping software development organisations:

1. describe the current state of software security in individual software products;

2. describe the target state of the software security in individual software products;

3. identify and prioritise opportunities for improvement in development and lifecycle management processes;

4. assess progress toward the target state; and

5. communicate among internal and external stakeholders about software security and security risks.

BSA accordingly **recommends that** the Australian government should consider the Secure Software Framework as a basis for encouraging "built in" cyber security through the 2020 Strategy. BSA is eager to work with the Australian government to explore how the Secure Software Framework can be best incorporated into the 2020 Strategy, and would welcome the opportunity to discuss this initiative further.

### Question 13: "*How could we approach instilling better trust in ICT supply chains?*"

Managing security risks to ICT supply chains is an important priority for both governments and businesses globally. Yet, mistargeted policy interventions aimed at improving security can introduce unintended consequences by causing severe damage to the technologies and economic activities they seek to protect. Effective government approaches to supply chain risk management recognise the global, interconnected nature of supply chains and the threats against them, identifying and disrupting malicious actors through policies and processes that are sustainable, reciprocal, and transparent.

As the Australian government seeks to address risk and thereby instil better trust in ICT supply chains, BSA **recommends that** the Australian government should consider adopting, as part of the 2020 Strategy, the following principles, which are described in the *BSA Principles for Good Governance: Supply Chain Risk Management*[16] (attached as **Annex C** to this submission), to guide effective government supply-chain risk management policies:

- Adopt **risk management** approaches to supply chain security that, among others, tailor mitigation strategies and prioritise actions based on the most relevant and potentially impactful risks, while fostering global technology competition.

[15] Available at: https://www.bsa.org/reports/bsa-framework-for-secure-software.

[16] Available at: https://www.bsa.org/policy-filings/bsa-principles-for-good-governance-supply-chain-risk-management.

- Embrace **interoperability** – consistency and compatibility of regulations and technical standards across national borders – to ensure that technology providers can develop, maintain, and secure innovative products across global boundaries and help to facilitate transnational operational collaboration against significant cyber threats.

- Ensure **transparency** in supply chain risk management policies and processes, including government disclosure to suppliers of identified supply chain vulnerabilities.

- Exercise **discretion** when addressing malicious threats and avoid systemic interventions in global supply chains.

- Pursue aggressive law **enforcement** against malicious actors.

- Undertake **collaboration** with key non-governmental stakeholders, including industry, in securing supply chains and developing best practices for supply chain risk management.

- Establish meaningful mechanisms to ensure **fairness** and due process in resolving disputes among stakeholders.

- Invest in **research and development** of new technological approaches to foster supply chain integrity.

## E. Conclusion

BSA commends the Australian government for its consultative process and strong engagement of the industry in developing Australia's 2020 Strategy, and thanks the Australian government again for this opportunity to make a submission on this important matter.

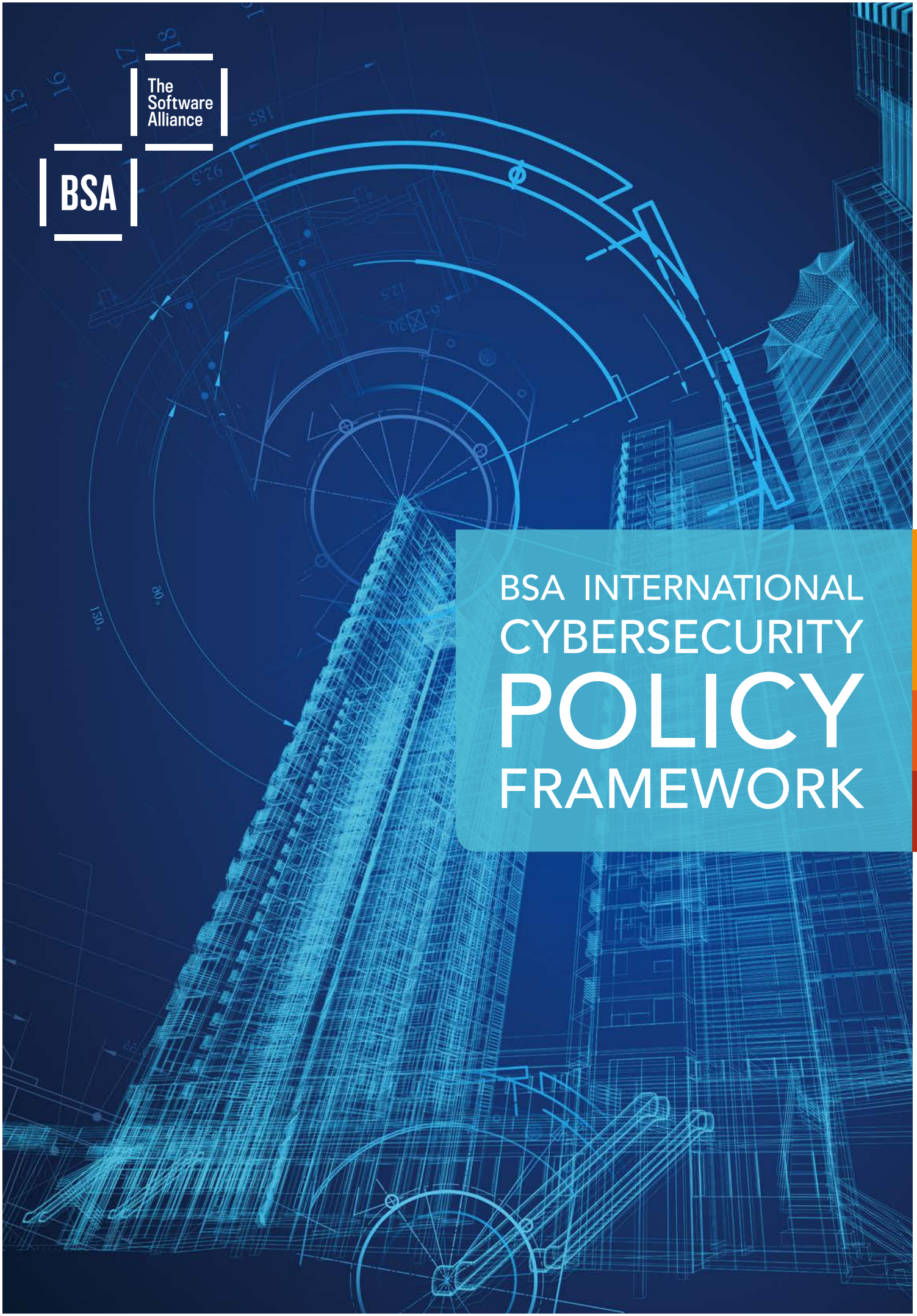
BSA and our members would be delighted to further engage with the Australian government to respond to any questions on this submission, and to explore ways in which BSA and our members can work with the Australian government and other stakeholders to develop an effective and balanced 2020 Strategy, including on how best to incorporate and operationalise the *BSA International Cybersecurity Policy Framework,* the *BSA Framework for Security Software*, and the *BSA Principles for Good Governance: Supply Chain Risk Management.*

If you require any clarification or further information in respect of this submission, please contact Mr Darryn Lim at darrynl@bsa.org or +65 6292 0680.

**BSA | The Software Alliance**

# Annex A

## BSA International Cybersecurity Framework


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 an Up-to-Date National Cybersecurity Incident Response Plan for Critical Infrastructure |
| | ✓ Craft Sector-Specific Plans as Appropriate |
| **Stakeholder Engagement** | ✓ Establish a Structure for Facilitating Public-Private Partnerships |
| | ✓ Create a Mechanism for Supporting Sub-National and Local Governments |
| **CYBERSECURITY AND THE GOVERNMENT** | |
| **Preparedness and Response** | ✓ Establish and Resource a National Computer Emergency Response Team |
| | ✓ Authorize and Encourage Timely Threat Information-Sharing |
| | ✓ Ensure a 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 a Risk-Based, Flexible Policy Framework |
| | ✗ Avoid an 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 |
| | ✓ 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 the 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

## 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).

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 to promote sharing of critical cybersecurity information across national stakeholders. The single national body assigned lead responsibility for cybersecurity will often serve as the NCA.

**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 a 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 a 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 a 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 among 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.

***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 rather than to stockpile, buy, sell, or exploit them.***

## 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

[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.

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.

**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 a 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 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 by 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

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.

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.

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.

***Certification regimes should emphasize software security-by-design principles by including process-based standards for software development.***

**Avoid an 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

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.

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 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 to discover and refine attack methods. Governments should avoid any law requiring the transfer of, or access to, source code 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. Although 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.

***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.***

**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

***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.***

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 the 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

[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.

> ***In strategy documents, organization, and budgets, governments should emphasize strong, collaborative cybersecurity as a critical element of national security and should develop and articulate clear areas of focus to promote cooperation.***

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 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 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."

**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."

**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."

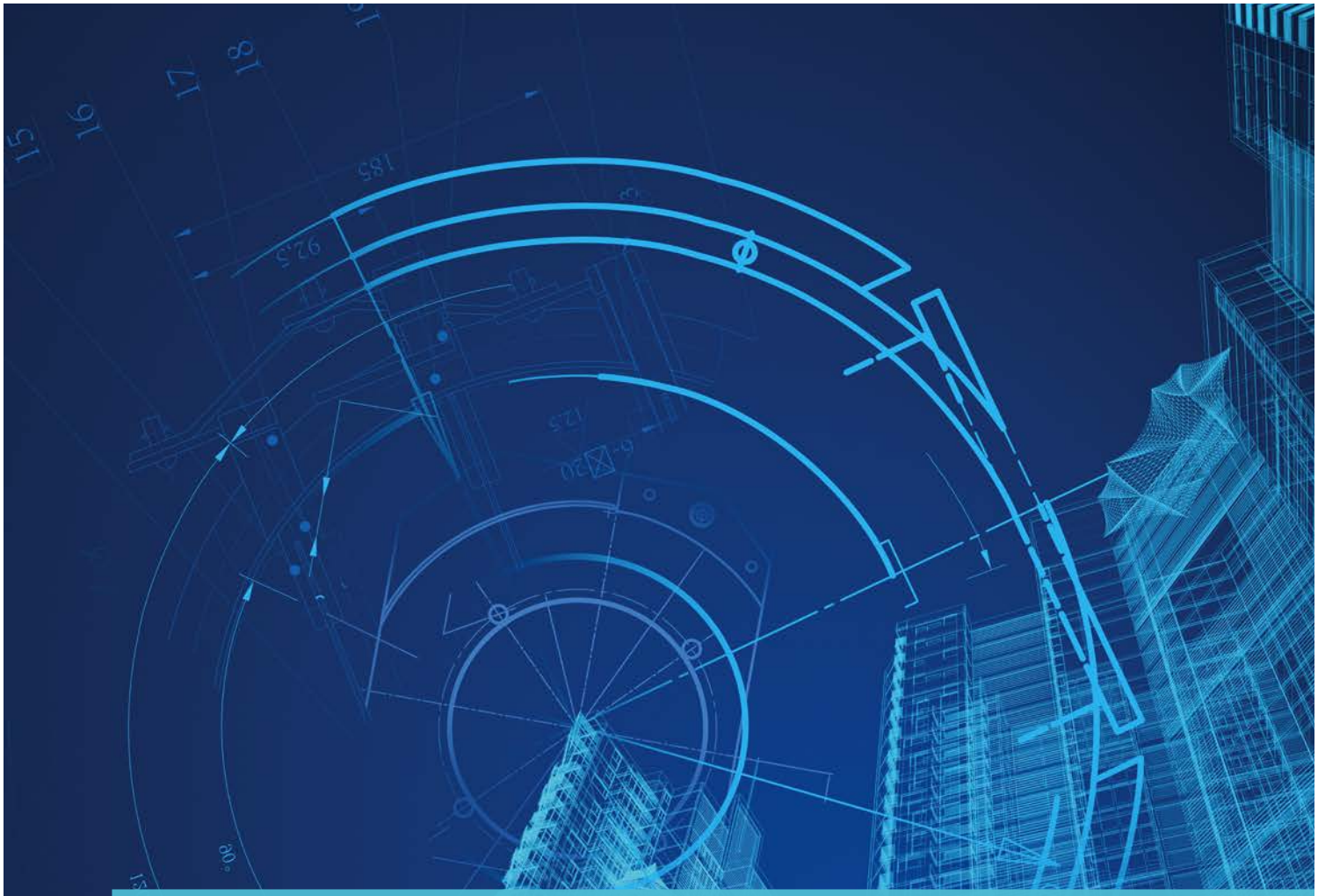
**Significant Cybersecurity Incident.** A significant cybersecurity incident may be defined as "a cybersecurity incident resulting in:

- 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


# Annex B

## BSA Framework for Secure Software

The Software Alliance

BSA

# The BSA Framework for Secure Software

## A NEW APPROACH TO SECURING THE SOFTWARE LIFECYCLE

# CONTENTS

# I. Executive Summary

Developments over the last several years have resulted in the dramatic expansion of software-powered capabilities from traditional computers and industrial control systems into diverse personal devices, widely deployed sensors, smart appliances, connected vehicles, robotic systems, and beyond. These innovations are driving the creation of a new, connected digital economy and can yield tremendous economic and social benefits. Yet, because these technologies also have the potential to create economic, legal, and even physical risk, software developers must have the joint goals of building software securely and ensuring that it can be securely maintained throughout its lifecycle.

Software development organizations, their customers, and policymakers are increasingly seeking ways of assessing and encouraging security across the software lifecycle. While standards and guidelines exist to aid and inform developers in achieving these goals, there is no consolidated framework that brings together best practices in a manner that can be effectively measured, regardless of the development environment or the purpose of the software. BSA | The Software Alliance has developed The BSA Framework for Secure Software (the "Framework") to fill that gap.

Specifically, the Framework is intended to be used to help software development organizations:

(1) describe the current state of software security in individual software products;

(2) describe the target state of software security in individual software products;

(3) identify and prioritize opportunities for improvement in development and lifecycle management processes;

(4) assess progress toward the target state; and

(5) communicate among internal and external stakeholders about software security and security risks.

The Framework is intended to focus on software products (including Software-as-a-Service) by considering both the process by which a software development organization develops and manages software products and the security capabilities of those products. It is intended to complement, rather than replace, guidance for organizational risk management processes. To the greatest extent possible, it seeks alignment with recognized international standards and to remain flexible, adaptable, outcome-focused, and risk-based.

The Framework is intended to become a living document, to be updated and improved based on ongoing feedback from BSA's members and other relevant stakeholders.

# II. Introduction

Modern society is built on software. Software powers personal technologies, critical infrastructure, scientific research, and industries across every sector. It drives emerging innovations such as the Internet of Things (IoT), blockchain, and artificial intelligence (AI). As software becomes increasingly central to our lives, making it secure and reliable becomes ever more critical in the face of an evolving and expansive cybersecurity threat landscape.

From within the software community, best practices are emerging that help software developers address important aspects of software security, including security-by-design principles, secure development lifecycle processes, and internationally recognized standards for key security elements such as identity management, encryption, and secure coding. Although attention to each specific security consideration can achieve marginal security gains, effective security requires a comprehensive and risk-informed approach that combines individual considerations into a holistic, lifecycle-long framework. And a comprehensive approach must be tailored to address the nuanced, diverse, and evolving challenges associated with different types of software and connected devices, from the "bare metal" to the most advanced.

Building on best practices pioneered by many of its members, BSA | The Software Alliance has developed a software security framework to bring consistency to these complex challenges. The BSA Framework for Secure Software is intended to establish an approach to software security that is flexible, adaptable, outcome-focused, risk-based, cost-effective, and repeatable. Eschewing a one-size-fits-all solution, this voluntary framework will provide a common organization and structure to capture multiple approaches to software security by identifying standards, guidelines, and practices that can help software development organizations achieve desired security outcomes while accounting for the wide spectrum of intended uses, risk profiles, and technological solutions among software products.

Recent technological developments illustrate the increasing ubiquity of software and the need for a flexible, comprehensive software security framework. Software-powered capabilities are rapidly expanding from desktop computers and industrial systems into nearly every corner of personal lives and business activities, including diverse personal devices, widespread sensors, smart appliances, diverse business applications, connected vehicles, and robots. As these capabilities evolve, software development is growing increasingly diverse and complex.

> ***The BSA Framework for Secure Software is intended to establish an approach to software security that is flexible, adaptable, outcome-focused, risk-based, cost-effective, and repeatable.***

Consider the different ways software is used in several emerging technologies:

### Internet of Things

Software is at the core of the IoT, and secure software must be at the core of IoT security. IoT devices, like other computing devices, have many different forms, functions, and levels of complexity. At the low end, some "bare metal" sensors lack even a basic operating system and contain only software code sufficient to perform one or two simple functions. More complex devices may include operating systems, AI algorithms, or the hundreds of millions of lines of code needed to operate many of today's connected vehicles. How can we achieve confidence in the security of software products across this spectrum?

### Software-as-a-Service (SaaS)

Many software applications are now being operated as services from a cloud-based architecture in which code is segmented across multiple container environments, updated constantly and in real-time, and accessed via Internet connections rather than installed locally. Some SaaS applications are updated dozens or even hundreds of times each day, with little or no disruption to the user experience. How can we craft a software security framework that accounts for the new technical approaches to software security that SaaS development may demand, while at the same time driving secure outcomes in traditional software development?

### Artificial Intelligence

AI also brings new considerations to software development, including new security challenges. AI software often integrates multiple software components, frameworks, and platforms, potentially introducing new risk with each additional element. Moreover, AI generally must ingest and process enormous data sets, introducing risk through the exposure of the data itself. Combined, these risks demonstrate the importance of software security for AI products. Yet, at the same time, AI products are creating promising new approaches to integrating security into software development. How can we address the risks — and harness the benefits — for security in AI software?

These diverse and constantly evolving software development techniques and products demonstrate the need for an outcome-focused approach that can consistently ensure security across a broad array of technical considerations. Additionally, static, inflexible approaches will either disrupt innovation or fail to keep pace with evolving threats because software is constantly changing.

The intent of the Framework is to provide the entire software industry with a comprehensive, adaptable, and relevant framework for software security. By adopting a flexible, outcome-focused approach rooted in industry best practices and international standards, the Framework is structured to be applicable to the entire spectrum of (1) software development organizations and vendors, from the individual entrepreneur to large-scale, multi-national businesses; (2) software development methods, from traditional to DevOps; and (3) software products, from simple IoT sensors to complex AI algorithms.

> ***Software security encompasses what a software development organization does to protect a software product and the associated critical data from vulnerabilities, internal and external threats, critical errors, or misconfigurations that can affect performance or expose data.***

## Defining "Software Security"

Software security encompasses what a software development organization does to protect a software product and the associated critical data from vulnerabilities, internal and external threats, critical errors, or misconfigurations that can affect performance or expose data. It comprises both organizational processes and product capabilities.

- **Organizational processes** include governance structures, strategies, guidance, and clearly defined procedures that guide the development of software in a manner that identifies and incorporates security objectives throughout a product's lifecycle, protects the integrity of the development environment, applies resources to incident and vulnerability management, and manages the supply chain that supports the software development project.

- **Product security capabilities** are technical aspects of specific software products that are useful in enabling the products to address common security challenges, such as protecting data, preventing unauthorized access or use, tracking incidents and vulnerabilities, and managing unforeseen events.

Both organizational processes and product security capabilities are vital elements of software security.

Software security is often discussed in relation to *software assurance*. Software assurance has been defined[1] as the "level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner." It has also been defined[2] as "the development and implementation of methods and processes for ensuring that software functions as intended and is free of design defects and implementation flaws." While such definitions may suggest that the level of security associated with a given software product could be ascertained simply by measuring the presence and extent of defects or vulnerabilities in its code base, software security is rarely that straightforward.

One challenge is that — at least currently — it is impractical to expect complex software code to be entirely free of vulnerabilities. Indeed, according to some estimates, software products currently average roughly 1–5 defects per 1,000 lines of code, with many complex software products incorporating tens or hundreds of millions of lines of code in total.[3] While defect-free code should always be a developer's goal, it is not a realistic industry standard. Instead, the goal should be the widespread adoption of practices and processes that minimize code defects, and particularly known software vulnerabilities, and to maintain a proactive security posture oriented to identifying and addressing problems before they can be exploited. In fact, researchers have documented substantial improvements in average software defect density among leading software developers through the implementation of secure development lifecycle approaches and other software security best practices.

A second challenge is that any approach to software security that is distilled into a test or series of tests at a single point in time is inherently flawed. As developers increasingly adopt iterative approaches to development, incorporate third-party components, and face evolving security threats, a software product may change continually and substantially over its lifecycle. Testing methodologies undergo evolution as well; for example, the set of known software vulnerabilities assessed by certain testing methodologies may be frequently updated to include newly discovered flaws. Security is a persistent requirement; while software testing is a critical element of secure development, it is not a stand-in for a sustained, security-focused approach to lifecycle management.

[1] https://www.hsdl.org/?view&did=7447

[2] https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf

[3] https://resources.sei.cmu.edu/asset_files/Webinar/2014_018_100_295971.pdf

Other models exist for informing or assessing software security. Some of these models, including SAFECode's *Fundamental Practices for Secure Software Development*, the Software Assurance Maturity Model, and various secure software development lifecycle methodologies, serve as important starting points for the Framework described in this document. They provide detailed guidance, informed by broad industry best practices, on a wide range of considerations organizations should address to maximize their ability to produce secure software in a verifiable, repeatable, transparent manner. However, in many cases, these guidance documents lack specificity and are primarily targeted toward organizations, focusing almost exclusively on organizational approaches, processes, and methodologies that collectively constitute the *input* of software development. They offer limited guidance on security considerations in relation to the *output* of software development; that is, the software product.

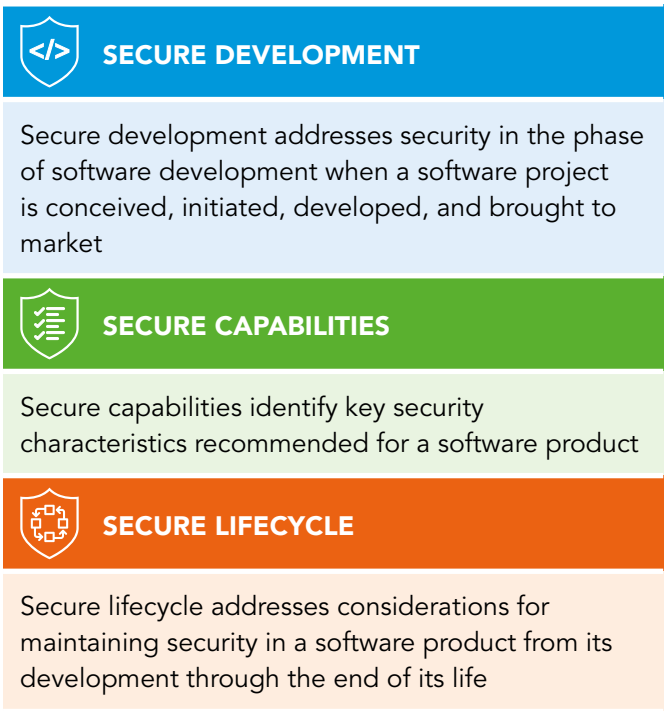
The Framework takes the approach of defining software security by considering both input and output; that is, it includes considerations of organizational processes that guide how vendors approach the development and maintenance of a software product as well as security capabilities and considerations relevant to the product itself. Moreover, it provides this guidance at a level of detail that is specific enough to be measurable, without compromising the flexibility necessary to ensure that all organizations can tailor the guidance according to the type, use, and associated risk of a software product.

The Framework is intended to apply to all types of software. Yet, because of the tremendous diversity in types of software, software development processes, and risks, some security considerations will be more relevant to certain types of software than others. Moreover, organizations will vary in how they customize approaches to achieving the outcomes described in the Framework. The Framework is intended as a tool to create a common language for discussions about how software approaches security, enabling stakeholders to hone in on the security outcomes most relevant to the circumstances. Rather than serving as a box-checking exercise, such a common language enables organizations to describe how they approach a specific security outcome or why that outcome may not be applicable to their product.

## Framework Basics

The Framework identifies best practices relating to both organizational processes and product capabilities across the entire software lifecycle. It is organized into six columns: Functions, Categories, Subcategories, Diagnostic Statements, Implementation Notes, and Informative References.

**Functions** organize fundamental software security activities at their highest level, consistent with the software lifecycle. The Functions are:




**Categories** divide a Function into distinct considerations and disciplines relevant to the Function. Many Categories are fundamentally interwoven with other Categories; for example, the "Vulnerability Management" and "Vulnerability Notification and Patching" Categories are conceptually closely related, as successful vulnerability management necessarily involves vulnerability notification and patching. However, the Categories seek to distill best practices into distinct subjects or disciplines; in this example, "Vulnerability Management" provides guidance for organizational processes to identify, prioritize, and mitigate vulnerabilities, whereas "Vulnerability Notification and Patching" identifies best practices for developing and issuing patches, mitigations, and notifications to customers. Categories within the same

> ***By "software development organizations," the Framework intends to address all parts of an organization involved in the design, development, deployment, and maintenance of software, recognizing that each organization must determine how it can assign roles and responsibilities to most effectively achieve desired security outcomes.***

Function may involve different communities of practices within the software development organization; for example, "Secure Coding" practices will may be most relevant to a different part of a software development team than those members responsible for "Supply Chain Risk Management" practices.

**Subcategories** further divide a Category into distinct, unitary concepts that express identified software security best practices.

**Diagnostic Statements** identify specific, verifiable outcomes. They provide a set of results that help support achievement of the outcomes in each Category. Diagnostic Statements are not intended as an exhaustive list of best practices, but as a set of desired outcomes that are universally relevant, to the maximum extent possible, to enhancing security across all classes and types of software. The Framework does not intend that every Diagnostic Statement will apply to every development environment or software product. Instead, through an examination of risk, software development organizations will apply the Diagnostic Statements appropriate for their environment and product, and identify cases in which Diagnostic Statements are inapplicable or irrelevant. This approach is consistent with other risk-based frameworks that seek to encourage and guide secure activities while avoiding becoming simple checklists.

**Implementation Notes** provide additional information, where necessary, such as examples of how organizations may achieve security outcomes described in the Diagnostic Statements, interpretations of how Diagnostic Statements may apply in different development environments, and guidance on aligning implementation with risk.

**Informative References** are additional resources that identify and describe best practices, guidelines, or further information for the implementation of an associated Diagnostic Statement. They may describe methods for achieving the described outcome, provide technical specifications or related best practices, and offer further clarity and specificity on the security benefits of the described outcome. Informative References include internationally recognized technical standards, best practice manuals and guidelines, and references to Common Weakness Enumerators (CWEs). A current list of CWEs is maintained at https://cwe.mitre.org/. In some cases, multiple standards may offer alternative approaches to achieve similar outcomes. Similarly, CWE references are drawn from a community-developed taxonomy of software weaknesses that serves as a common language for describing weaknesses and provides a baseline for identification, mitigation, and prevention of such weaknesses. Numerous CWE references may be related in some form to a specific Diagnostic Statement; the Framework attempts to identify the most relevant weaknesses resulting when the Diagnostic Statement is incompletely or improperly addressed. In all cases, Informative References are illustrative and are not intended to be either exhaustive or prescriptive.

The Framework's Subcategories and Diagnostic Statements are often focused on the individuals and team that actually develop software. In practice, entities developing software are complex organizations that often include separate software development teams that interact with security teams, corporate governance structures, and external requirements, each of which play key roles in driving the security outcomes the Framework describes. By "software development organizations," the Framework intends to address all parts of an organization involved in the design, development, deployment, and maintenance of software, recognizing that each organization must determine how it can assign roles and responsibilities to most effectively achieve desired security outcomes.

## Framework Purpose

The Framework is intended to be used to help software development organizations:

1. Describe the current state of software security in individual software products.
2. Describe the target state of software security in individual software products.
3. Identify and prioritize opportunities for improvement in development and lifecycle management processes.
4. Assess progress toward the target state.
5. Communicate among internal and external stakeholders about software security and security risks.

The Framework is intended to focus on software products (including Software-as-a-Service), by considering both the process by which a software development organization develops and manages software products and the security capabilities of products. It is intended to complement, rather than replace, guidance for organizational risk management processes. To the greatest extent possible, it seeks alignment with recognized international standards.

The Framework is intended to become a living document, to be updated and improved based on ongoing feedback from BSA's members and other relevant stakeholders.

## Guiding Principles

The Framework is based on five key principles:

- Risk-based
- Outcome-focused
- Flexible
- Adaptable
- Aligned with Internationally Recognized Standards

### *Risk-Based.*

Software is enormously diverse, ranging from applications that perform only a few basic functions to highly sophisticated AI programs, and it is used in an enormously diverse array of contexts, from home computing networks to the very backbone of the Internet. The different types and uses of software carry different risks; for example, the software behind a mobile phone game may pose far less threat to cyber or physical security than the software operating an electricity grid's control system.

To manage the risks associated with software, organizations should build software development processes around careful analysis of the risks associated with their products, the potential resulting impacts, and their organization's risk tolerance. With an understanding of risk tolerance, organizations can prioritize security activities in their software development and lifecycle management processes, enabling informed decisions about where to prioritize improvements and how to align financial and human resources.

> ***Many elements of the Framework are intentionally structured to provide software development organizations with the flexibility to tailor their approaches based on the risk profile of the product.***

Risk informs the Framework throughout its three functions and is intended to guide software development organizations and vendors to address security considerations in operational processes and product security capabilities according to the level of risk associated with the product.

For example, consider the first Subcategory articulated in the Framework which reads: "Threat modeling and risk analysis are employed during software design to identify threats and potential mitigations." This risk analysis is designed to guide software development organizations toward adopting the security controls most appropriate to the type and uses of their products. Understanding of the risk subsequently informs the development of a plan to address security considerations in the software's development and deployment.

## *Outcome-Focused.*

The Framework communicates best practices in their most detailed form through Diagnostic Statements that identify specific, measurable outcomes. These statements are intended to be neutral with respect to coding language, development process, and technical approach. Rather than dictating specific security techniques, the Framework focuses on the outcomes software development organizations and vendors ideally should achieve to enhance the security profile of the software.

## *Flexible.*

Software development as a discipline is constantly evolving based on innovations in efficiency and management, emerging customer demands, new approaches to coding languages or software development tools, and technical breakthroughs. Moreover, cybersecurity requires constant innovation to keep pace with changing threats. Any approach to software security must be flexible enough to enable software developers to develop new approaches to new challenges, and to deliver innovative products to the customers who depend on them.

The Framework approaches this vital principle by ensuring that it specifies outcomes that are neutral with regard to coding language, development process, and technical approach. Similarly, the Framework recognizes that some Diagnostic Statements may be more important to some organizations than others. For example, companies securing SaaS products will find statements relating to securing containers, such as TC.1-6, more applicable to their software development environment than businesses providing mostly out-of-the-box software. Likewise, organizations developing out-of-the-box software may find Diagnostic Statements relating to anti-tamper techniques, like SM.4-1, more useful. The Framework is structured in a way such that each Diagnostic Statement is intended to maintain flexibility while remaining applicable to software of all types, languages, and development processes.

Many elements of the Framework are intentionally structured to provide software development organizations with the flexibility to tailor their approaches based on the risk profile of the product. For example, the "Support for Identity Management and Authentication (SI)" category recognizes that not all software products will require an identity management and authentication mechanism but includes clear guidelines for those that do. It directs that software "avoids hard-coded passwords" and "avoids authentication mechanisms that allow insufficiently complex passwords, insufficient password aging management, unlimited log-on attempts, commonly used password topologies, or unverified password changes." For some software products, these guidelines will mean adopting strong identity management and authentication mechanisms, such as multi-factor authentication, single sign-on technologies, and log-on limits. For others, they will mean ensuring that third-party identity management and authentication tools meet those guidelines before they are incorporated. For still others, they will mean validating that such measures are not needed based on the product's risk and architecture.

**EXAMPLE**

### Preventing SQL Injection Attacks.

Hackers may use SQL injection — a code injection technique in which malicious SQL statements are inserted into an entry field for execution — to compromise the confidentiality, integrity, and/or availability of data used in a software program. SQL injection attacks are particularly common in database-driven applications and are among the common types of malicious cyber activity.

Concatenation of untrusted data with string constants (string concatenation, or the combining of multiple strings of untrusted data into a single string) is a common and dangerous weakness that SQL injection attacks can take advantage of. To mitigate the risk of SQL injection attacks, the Framework includes the following diagnostic statements in the **Secure Coding** category of the **Secure Development** function:

> **SC.3-1. Software avoids, or includes documented mitigations for, known security vulnerabilities in included functions and libraries.**
>
> **SC.3-2. Software development organizations validate input and output to mitigate common vulnerabilities in software.**

By focusing on secure outcomes, the Framework avoids mandating specific technical approaches to structuring SQL statements, such as prescribing certain stored procedures or whitelisting techniques. SQL statements can be created and parameterized using many different programming languages, libraries, and frameworks; the Framework establishes clear security outcomes that are targeted and meaningful but retains the flexibility to enable its achievement through each of these differing languages, libraries, and frameworks. In each case, the outcome specified in the diagnostic statement is linked to references to informative material that provides further detail on achieving the outcome, including references specifying techniques to prevent SQL injection attacks.

Not all software products are at risk of SQL injection attacks, and not all software products utilize dynamic SQL statements. The security outcomes specified by the Framework are met equally by the software product that develops properly parameterized SQL statements as by the software product that excludes dynamic SQL statements altogether. The appropriate approach to meeting the specified security outcome will be based on a risk-informed software design and security architecture.

## *Adaptable.*

In today's development context, software is constantly changing. Many products are continually updated with new features and additional security measures long after their original market deployment. For that reason, software security must be conceptualized in a way that is adaptable to this lifecycle, as well as to the constant innovation of new technologies, processes, and standards in the software industry. For that reason, approaches to software security that mandate specific technical measures or that endeavor to subject software products to batteries of tests that assess security at a single point in time will fail to keep pace with the constant evolution of software. Instead, this Framework provides a tool to assess the characteristics of software security throughout a software product's lifecycle, using outcome-focused diagnostic statements that are adaptable to diverse and evolving technical approaches.

**EXAMPLE**

### Vulnerability Advisories to SaaS Customers.

To ensure that users are properly informed of relevant security information associated with software updates, the **Vulnerability Notification and Patching** category of the **Secure Lifecyle** function includes the following diagnostic statement:

> **VN.3-1. Users are notified of a significant security issue when a remediation is in place for each supported version of the affected product.**

As important as such notifications can be when users are asked to install updates that could potentially have broader impacts to their own devices or systems, it may not be feasible for notifications to accompany every software update in some contexts. For example, many SaaS vendors operate in a continuous delivery environment, meaning software is produced in short cycles of testing, staging, pre-production, and production. Because SaaS is a web-based model in which software is maintained on remote servers rather than installed on user devices, SaaS software updates are also generally not installed on user devices. Continuous integration and continuous delivery methodologies make it possible to quickly deploy new versions of, or security updates to, a SaaS application without customer disruptions or losses of service. Sophisticated SaaS vendors may deploy dozens, or even hundreds, of software updates to an application each day.

By focusing on information relevant to *significant* security issues, the Framework avoids onerous notification requirements, which may be impossible to meet in a SaaS environment, while ensuring customers are well-informed regarding the security of their products and services.

### *Aligned with Internationally Recognized Standards.*

Internationally recognized technical standards provide widely vetted, consensus-based information and guidance for defining and implementing effective approaches to cybersecurity and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. Industry leaders have developed a range of international standards and best practices for secure-by-design software development. To ensure international interoperability and express consensus best practices, the Framework seeks to align, to the greatest extent possible, with internationally recognized technical standards wherever they exist. Currently, the most notable example relevant to secure software development is the ISO/IEC 27034 series of standards, which sets out guidance on "integrating security seamlessly throughout the lifecycle" of software applications.

## Implementing the Framework for Secure Software

The Framework is designed to support the systematic processes used by software development organizations to identify, assess, and minimize cybersecurity risk throughout the lifecycle of software products. Using the Framework as a cybersecurity risk management tool, an organization can establish a holistic secure development lifecycle that identifies likely risks, enables conscientious decisions about risk mitigation and risk tolerance, improves software quality, and prepares the organization to address emerging security considerations throughout the software's lifecycle.

> ***Using the Framework as a cybersecurity risk management tool, an organization can establish a holistic secure development lifecycle that identifies likely risks, enables conscientious decisions about risk mitigation and risk tolerance, improves software quality, and prepares the organization to address emerging security considerations throughout the software's lifecycle.***

Specifically, software development organizations may find the Framework to be a useful tool for the following purposes, among others:

- **Development process guidance.** A software development organization should publish definitive direction on the policies and processes that development of a new software product is expected to follow in order to ensure that all involved stakeholders understand roles, responsibilities, and expectations. Organizations may choose to amend software development processes and process guidance to ensure the elements of the Framework are accounted for throughout the product development lifecycle.
- **Training and awareness.** A software development organization may consider developing internal training and education programs to build a culture of security and to ensure that stakeholders are trained in responsibilities and methodologies appropriate to their roles in the software development lifecycle. Organizations may choose to incorporate elements of the Framework into internal training and awareness modules. In addition, the Framework may provide a useful tool for educating executives about how security is addressed in the development process, how resources are aligned to security considerations, and how individual products incorporate cybersecurity.
- **Tracking and assessment.** Software development organizations may wish to use the Framework as a tool to track a product as it is developed or to assess its security profile according to concrete metrics. For example, software development lifecycles often establish release gates that require a project to meet an established measure or obtain a waiver before advancing; elements of the Framework may be incorporated into release gate criteria. Additionally, the Framework may help an organization identify metrics that define and measure software security for its products.
- **Vendor relations.** A software development organization should implement measures to ensure the integrity of its supply chain. Organizations may choose to use the Framework to guide purchasing decisions and/or the development of vendor contracts that ensure third-party software components will not jeopardize the organization's security objectives and compliance requirements.
- **Public security narrative.** Software development organizations may wish to communicate information about a product's security features and its approach to mitigating cybersecurity risk to a public audience. The Framework may be useful in enabling organizations to build a narrative about their secure development lifecycle and product security.

# III. BSA Framework for Secure Software

*The Framework does not intend that every Diagnostic Statement will apply to every development environment or software product. Software development organizations will identify and apply the Diagnostic Statements appropriate for their environment and product based on analysis of risk.*

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Secure Coding (SC)** | **SC.1.** Threat modeling and risk analysis are employed during software design to identify threats and potential mitigations. | **SC.1-1.** Software development organizations document likely threats. | Threat modeling attempts to identify and prioritize the potential threats against a software product or component in order to guide software development decisions that defend against identified threats. Some software developers work in accordance with "zero trust" principles, which assume a pervasively hostile environment. Yet, even with zero trust approaches, threat modeling is important for identifying sensitive data and prioritizing threats for mitigation. Developers should consider the risk profile of the product when determining the level of detail to provide in such documentation. | ISO/IEC 27034; OWASP Application Security Verification Standard; SAFECode "Fundamental Practices"; SAFECode "Tactical Threat Modeling"; SAMM; BSIMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet |
| | | **SC.1-2.** Threats are rated and prioritized according to risk. | | ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet |
| | | **SC.1-3.** Software development organizations apply common threat modeling methodologies. | | ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet; SAFECode "Tactical Threat Modeling" |
| | | **SC.1-4.** Compensating controls are identified and mapped to threats. | | ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Secure Coding (SC)** *(continued)* | **SC.2.** Software is developed according to recognized, enforceable coding standards. | **SC.2-1.** Standards are formally identified and documented. | | ISO/IEC TS 17961; SEI CERT C Coding Standard; SEI CERT C++ Coding Standard; SEI CERT Java Coding Standard; NCSC |
| | | **SC.2-2.** Software uses canonical data formats. | | SAFECode "Fundamental Practices"; CWE-21; CWE-22; CWE-35; CWE-36; CWE-37; CWE-38; CWE-39; CWE-40 |
| | **SC.3.** The software is secure against known vulnerabilities, unsafe functions, and unsafe libraries. | **SC.3-1.** Software avoids, or includes documented mitigations for, known security vulnerabilities in included functions and libraries. | Software should avoid known vulnerabilities to the greatest extent possible. In some instances, there may be reasons for software to incorporate functions or libraries known to include vulnerabilities; such functions or libraries should only be incorporated when developers include documented mitigations that ensure the vulnerabilities are not exploitable. | NIST NVD; CWE/SANS Top 25 Most Dangerous Software Errors; OWASP Top 10; CWE-1006; CWE-242 |
| | | **SC.3-2.** Software validates input and output to mitigate common vulnerabilities in software. | | SAFECode "Fundamental Practices"; OWASP Input Validation Cheat Sheet; CWE-20; CWE-89; CWE-119; CWE-120; CWE-183; CWE-184; CWE-242; CWE-625; CWE-675; CWE-805 |
| | | **SC.3-3.** Software encodes data and/or uses anti-cross site scripting (XSS) libraries. | | SAFECode "Fundamental Practices"; CWE-79 |
| | **SC.4.** Standard software assurance measures are employed in the software architecture and design. | **SC.4-1.** The software employs segmentation through sandboxing, containerization, or similar methodologies. | | SAFECode "Fundamental Practices"; CWE-265 |
| | | **SC.4-2.** The software employs fault isolation mechanisms. | | DoD-PPP |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Secure Coding (SC)** *(continued)* | **SC.4.** Standard software assurance measures are employed in the software architecture and design. | **SC.4-3.** The software employs system element isolation mechanisms. | | DoD-PPP; OWASP Application Security Verification Standard |
| | | **SC.4-4.** Software uses robust integer operations for dynamic memory allocations and array offsets. | Where errors in integer computation cannot result in security-relevant errors, use of robust integer operations may not be necessary. | SAFECode "Fundamental Practices"; CWE-129; CWE-131; CWE-190; CWE-680; CWE-805 |
| **Testing and Verification (TV)** | **TV.1.** Analysis and validation of the software attack surface is conducted. | **TV.1-1.** Attack surface is identified and mapped. | | OWASP Attack Surface Analysis Cheat Sheet, SAMM |
| | | **TV.1-2.** Analysis is informed by threat model(s) and risk analysis. | | SAFECode "Fundamental Practices"; OWASP Attack Surface Analysis Cheat Sheet |
| | **TV.2.** Code review using manual and/or automated tools is conducted. | **TV.2-1.** Code review release gates are established to guide software development. | To the extent possible, automated tools should be implemented and integrated with the software development process to ensure rigor and consistency. Manual tools can be substituted in cases where automation isn't feasible. | SAFECode "Fundamental Practices"; BSIMM; SAMM; OWASP Testing Guide; OWASP Code Review Guide |
| | **TV.3.** A comprehensive test plan for testing the functionality and security of software is established. | **TV.3-1.** Test plan is based on threat model(s) and risk analysis. | | SAFECode "Fundamental Practices"; OWASP Testing Guide |
| | | **TV.3-2.** The software is tested in a least privilege environment. | | SAFECode "Fundamental Practices" |
| | **TV.4.** Software security controls are properly tested with appropriate techniques. | | | ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; BSIMM; OWASP Testing Guide |
| | **TV.5.** Software is subjected to adversarial security testing techniques. | **TV.5-1.** Software development organizations establish security testing release gates. | | SAFECode "Fundamental Practices"; SAMM |
| | | **TV.5-2.** Software is subjected to penetration testing. | | ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; BSIMM; OWASP Testing Guide |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Process and Documentation (PD)** | **PD.1.** Secure development processes are documented throughout software development. | **PD.1-1.** Security requirements for the software are gathered from stakeholders and documented. | Developers should consider the risk profile of the product when determining the level of detail to provide in such documentation. | SAMM; Microsoft SDL |
| | | **PD.1-2.** Security guidance for the development of the software is documented. | | SAMM; Microsoft SDL |
| | | **PD.1-3.** Security guidance for the development of software is updated to reflect the results of root cause analyses of new vulnerabilities. | | SAFECode "Fundamental Practices"; BSIMM |
| | | **PD.1-4.** Security documentation outlining best practices for software use by end-users and developers is made available electronically. | | Microsoft SDL |
| | | **PD.1-5.** Testing and validation activities, including results, are documented. | | SAFECode "Fundamental Practices"; NIST IR 7622 |
| | | **PD.1-6.** Software development organizations maintain an up-to-date product history that documents changes to elements and configurations. | Depending on the development process, software developers may opt to maintain changelogs or change histories manually, or use automated tools such as project management software, source code management tools, and configuration management tools. It is increasingly recognized as a best practice for software developers to use automated tools that are capable of tracking the origin of code (date, time, rationale, responsible individual) on a line-by-line basis. Developers should consider the risk profile of the product when determining the level of detail to provide in such documentation. | |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Process and Documentation (PD)** | **PD.2.** Software development personnel are accountable for software security. | **PD.2-1.** A security advisor is assigned to the software development team. | | Microsoft SDL |
| | | **PD.2-2.** Software development personnel are trained on identified coding standards and role-specific best practices. | | BSIMM; SAMM |
| **Supply Chain (SM)** | **SM.1.** Software development is informed by supply chain risk management. | **SM.1-1.** An organizational supply chain management plan and processes for identification and reporting of supply chain incidents are established. | | NIST IR 7622; NIST SP 800-53 |
| | **SM.2.** Approved acquisition measures are in place to ensure the visibility, traceability, and security of third-party components. | **SM.2-1.** Information about providers of third-party components is identified and collected. | Relevant information may include the provider's processes for controlling access to software components, product development and testing standards, supply chain risk management practices, development environment, and vulnerability management processes. | SAFECode "Software Supply Chain Integrity Framework"; BSIMM; NIST Interagency Report 7622; NIST SP 800-53; CWE-505; CWE-506; CWE-507; CWE-510; CWE-511 |
| | | **SM.2-2.** Software development organization employs measures to document and, to the extent feasible, trace to their original source all third-party components directly acquired and incorporated into the software by the developer. | | SAFECode "Software Supply Chain Integrity Framework"; NIST IR 7622; NIST SP 800-53; CWE-505; CWE-506; CWE-507; CWE-510; CWE-511 |
| | | **SM.2-3.** To the maximum feasible through the use of manual and automated technologies, subcomponents integrated in third-party components are documented, and their lineage and dependencies traced. | | SAFECode "Software Supply Chain Integrity Framework"; NIST IR 7622; NIST SP 800-53; CWE-505; CWE-506; CWE-507; CWE-510; CWE-511 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Supply Chain (SM)** *(continued)* | **SM.2.** Approved acquisition measures are in place to ensure the visibility, traceability, and security of third-party components. | **SM.2-4.** Security requirements are incorporated into contracts, policies, and standards for vendors supplying software components. | | SAMM; BSIMM; NIST IR 7622; NIST SP 800-53 |
| | **SM.3.** Supply chain data — including information about software elements, design, testing, evaluation, threat assessments, delivery processes, and agreements language — is protected against unauthorized disclosure, access, modification, dissemination, destruction, and use. | **SM.3-1.** Supply chain data is protected at rest. | | NIST IR 7622 |
| | | **SM.3-2.** Supply chain data is protected in transit against unauthorized access. | | NIST IR 7622 |
| | **SM.4.** Software incorporates measures to prevent counterfeiting and tampering. | **SM.4-1.** Software includes mechanisms to ensure the integrity of the software, such as code-signing, anti-reverse engineering, or anti-tamper mechanisms. | | SAMM; BSIMM; NIST IR 7622; NIST SP 800-53 |
| | | **SM.4-2.** Software includes supplier source certification or authentication indicators and protects those indicators against tampering and counterfeiting. | | BSIMM; NIST IR 7622 |
| | | **SM.4-3.** Identification markers unique to the software's specific version are applied to each delivered product. | | NIST IR 7622; BSIMM; NIST SP 800-53 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Supply Chain (SM)** *(continued)* | **SM.5.** The software is identifiable through clear, discoverable information communicated in a standardized format. | **SM.5-1.** The software includes descriptive information about the software's identity. | Descriptive information should generally include the software's name, creator, version, licensing details and, where possible, information about the software's dependencies. | ISO/IEC 19770-2; SPDX Version 2.1; NIST IR 8060 |
| | **SM.6.** Deployment procedures ensure that the proper usages of software are established. | **SM.6-1.** The software includes mechanisms to reduce the likelihood that it is installed on unauthorized hardware or by unauthorized users, such as validating code-signing, authentication, or credentialing. | | NIST IR 7622 |
| **Tool Chain (TC)** | **TC.1.** Software is developed using tools configured for security. | **TC.1-1.** Software is developed using up-to-date versions of all tools and platform elements within the development environment. | | SAFECode "Fundamental Practices"; Microsoft SDL; OWASP C-Based Tool Chain Hardening Cheat Sheet; CWE-691; CWE-908 |
| | | **TC.1-2.** Development frameworks used in developing software use secure configurations. | | NCSC |
| | | **TC.1-3.** Compilers are configured to prevent common vulnerabilities and weaknesses. | | Microsoft SDL; OWASP Development Guide; CWE-1038 |
| | | **TC.1-4.** Compilers are configured to avoid unintentional removal or modification of security-critical code. | | Microsoft SDL; OWASP Development Guide; CWE-733; CWE-1038 |
| | | **TC.1-5.** Compilers are configured to automatically add defense code. | | Microsoft SDL; OWASP Development Guide; CWE-1038 |
| | | **TC.1-6.** Containers and other virtualization technologies used in deploying the software use secure configurations. | | BSIMM |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE DEVELOPMENT** | | | | |
| **Identity and Access Management (IA)** | **IA.1.** Throughout the supply chain and product lifecycle, the software development environment uniquely identifies and authenticates users and operators. | **IA.1-1.** Strong authentication methods are required for access to the development environment. | Strong authentication is generally understood to describe mechanisms that require authentication factors from at least two of three categories (knowledge, or something a user knows; ownership, or something a user has; and inherence, or something a user is), but may also utilize contextual information (e.g., geolocation or device information) and other factors to confirm a user's identity. Diagnostic Statements in the IA Category address identity and access management in the development environment. See the SI and AA Categories for information regarding security capabilities in software products themselves. | NCSC: NIST SP 800-53; NIST IR 7622 |
| | | **IA.1-2.** User and operator credentials are stored securely and revoked or disabled when no longer needed. | | NCSC |
| | **IA.2.** Policies to control access to data and processes for all users and operators are developed, documented, and applied throughout the development environment. | **IA.2-1.** Specific access controls for creation, read access, update, deletion, and execution are applied based on clearly identified and approved user and operator roles. | | SAMM; DHS/DACS |
| | | **IA.2-2.** Access controls are set for individual users and operators that provide only the necessary privileges required to perform an assigned task and only for the necessary time required to perform it. | | SAMM; DHS/DACS; DoD-PPP |
| | | **IA.2-3.** Unauthorized changes or deletions to code, development artifacts, and tools are prevented and logged. | | OWASP Logging Cheat Sheet; DHS/DACS; NIST IR 7622; CWE-778 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE CAPABILITIES** | | | | |
| **Support for Identity Management and Authentication (SI)** | **SI.1.** The software avoids architectural weaknesses that create risk of authentication failure. | **SI.1-1.** The software avoids hard-coded passwords. | | ISO/IEC 9798; OWASP Authentication Cheat Sheet; CWE-259; CWE-798 |
| | | **SI.1-2.** Software source code does not contain secrets. | Secrets may include credentials or keys. | |
| | | **SI.1-3.** Authentication mechanisms used by the software employ typical security techniques and avoid common security weaknesses. | Typical techniques and common weaknesses are rapidly evolving; software development organizations should stay abreast of current best practices. Current common security weaknesses include allowing insufficiently complex passwords, insufficient password aging management, unlimited log-on attempts, commonly used password topologies, and unverified password changes. | ISO/IEC 9798; OWASP Authentication Cheat Sheet; NIST SP 800-63; CWE-521; CWE-262; CWE-263; CWE-620; CWE-308 |
| | | **SI.1-4.** The software does not store sensitive authentication information, which may include passwords or keys, in source code or publicly accessible infrastructure. | | NCSC |
| | | **SI.1-5.** Any passwords or sensitive authentication information stored by the software is stored in accordance with current best practices. | Best practices for password storage are rapidly evolving; software development organizations should stay abreast of current best practices. | OWASP Password Storage Cheat Sheet |
| | **SI.2.** The software supports strong identity management and authentication. | **SI.2-1.** The software implements features, configurations, and protocols that establish or support standard, tested authentication services. | | ISO/IEC 9798; SAFECode "Fundamental Practices" |
| | | **SI.2-2.** The software is interoperable with applicable common industry standards for identity management and authentication. | | OAuth 2.0; OIDC; SAML 2.0; WS-FED; UAF; U2F; SAFECode "Fundamental Practices" |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE CAPABILITIES** | | | | |
| **Support for Identity Management and Authentication (SI)** *(continued)* | **SI.2.** The software supports strong identity management and authentication. | **SI.2-3.** Authentication controls fail securely. | When authentication controls fail securely, they prevent access by unauthenticated users even after encountering an error. | OWASP Secure Coding Practices |
| **Patchability (PA)** | **PA.1.** Software is capable of receiving secure updates and security patches. | **PA.1-1.** Software is capable of validating the integrity of a transmitted patch or update. | The Patchability category refers to technical aspects relating to the ability of the software to receive secure updates and patches. Activities of software developers relating to the development and dissemination of updates and patches are discussed in the Secure Lifecycle function. | NTIA "Voluntary Framework for Enhancing Update Process Security"; NIST SP 800-147; CWE-924 |
| | | **PA.1-2.** Software includes a mechanism to notify end users of patch or update installation. | | NTIA "Voluntary Framework for Enhancing Update Process Security" |
| | | **PA.1-3.** Software reverts to a known-good state upon failed installation of updates or security patches. | | NTIA "Voluntary Framework for Enhancing Update Process Security" |
| **Encryption (EN)** | **EN.1.** Software is developed in accordance with an encryption strategy that defines what data should be encrypted and which encryption mechanisms should be used. | **EN.1-1.** Software enables the use of encryption to protect sensitive data from unauthorized disclosure. | | SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-311 |
| | | **EN.1-2.** Software enables the use of encryption to protect the software itself from tampering. | | |
| | | **EN.1-3.** Software does not expose sensitive data upon failure of encryption mechanisms. | | OWASP Secure Coding Practices; CWE-636; FIPS 140-2 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE CAPABILITIES** | | | | |
| **Encryption (EN)** *(continued)* | **EN.2.** Software avoids weak encryption. | **EN.2-1.** Software avoids custom encryption algorithms and implementations. | In unique circumstances when a developer identifies a need to use a custom algorithm or implementation, the developer should establish and document a robust procedure to validate the security of the custom algorithm or implementation prior to deployment. | ISO/IEC 18033-1; ISO/IEC 19790; FIPS 140-2; FIPS 186-4; FIPS 197; FIPS 202; SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-325; CWE-326; CWE-327 |
| | | **EN.2-2.** Software enables the use of authenticated encryption. | | ISO/IEC 19772; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-326; CWE-327 |
| | | **EN.2-3.** Encryption employed by the software enables strong algorithms. | Standards for strong algorithms change over time; in general, strong algorithms will have no structural weaknesses, will maintain key sizes of sufficient length to defeat brute force attacks, and will have been standardized and deployed across a reasonably sized user base. | ISO/IEC 18033-1; ISO/IEC 19790; FIPS 140-2; FIPS 186-4; FIPS 197; FIPS 202; SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-326; CWE-327; CWE-330; CWE-331; CWE-338 |
| | | **EN.2-4.** Encryption employed by the software enables strong key lengths. | Standards for strong key lengths will change over time based on advancements in computing power and factoring techniques; in general, strong key lengths are of sufficient length to ensure brute force attacks are infeasible. | ISO/IEC 18033-1; ISO/IEC 19790; FIPS 140-2; FIPS 186-4; FIPS 197; FIPS 202; SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-326; CWE-327; CWE-330; CWE-331; CWE-338 |
| | | **EN.2-5.** Encryption capabilities employed by the software are configured to select strong cipher modes and exclude weak ciphers by default. | | ISO/IEC 18033-1; ISO/IEC 19790; FIPS 140-2; FIPS 186-4; FIPS 197; FIPS 202; SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-326; CWE-327; CWE-330; CWE-331; CWE-338 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE CAPABILITIES** | | | | |
| **Encryption (EN)** *(continued)* | **EN.2.** Software avoids weak encryption. | **EN.2-6.** Software is configured to disable or prevent the use of weak encryption algorithms and key lengths. | It may be necessary for software to support weak encryption algorithms and key lengths for reasons of backward compatibility. Where such support is required, the implementation should be carefully engineered and thoroughly reviewed to ensure that it does not allow an attacker to bypass the default or user selection of strong encryption. | CWE-326; CWE-327; CWE-330; CWE-331; CWE-338 |
| | **EN.3.** Software protects and validates encryption keys. | **EN.3-1.** Software ensures that cryptographic keys can be securely stored and managed, separate from encrypted data. | | ISO/IEC 18033-1; ISO/IEC 19790; FIPS 140-2; FIPS 186-4; FIPS 197; FIPS 202; SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57 |
| | | **EN.3-2.** Software includes a mechanism to manage key and certificate lifecycles. | Mechanisms for managing key and certificate lifecycles may include use of third-party key management systems. | ISO/IEC 18033-1; ISO/IEC 19790; FIPS 140-2; FIPS 186-4; FIPS 197; FIPS 202; SAFECode "Fundamental Practices"; OWASP Cryptographic Storage Cheat Sheet; NIST SP 800-57; CWE-324 |
| | | **EN.3-3.** Software includes a mechanism to validate certificates. | Not all software uses certificates; however, it is imperative that software that does use certificates is able to validate the authenticity of those certificates. This diagnostic statement should be applied consistent with the encryption strategy described in EN.1. | OWASP Cryptographic Storage Cheat Sheet; CWE-347 |
| **Authorization and Access Controls (AA)** | **AA.1.** Software design reflects the principle of least privilege. | **AA.1-1.** The software operates using only those privileges or permissions necessary for software to run correctly. | | SAFECode "Fundamental Practices"; DoD-PPD; CWE-250; CWE-271; CWE-272; CWE-274 |
| | | **AA.1-2.** Privileges are set in a configuration that is resistant to unauthorized changes. | | SAFECode "Fundamental Practices"; DoD-PPD; CWE-250 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE CAPABILITIES** | | | | |
| **Authorization and Access Controls (AA)** *(continued)* | **AA.1.** Software design reflects the principle of least privilege. | **AA.1-3.** An authorization strategy that applies authorization policies, access controls, and design principles to classes of data is implemented in the software. | | SAFECode "Fundamental Practices"; CWE-285; CWE-862; CWE-863 |
| | **AA.2.** The software's design supports authorization and access controls. | **AA.2-1.** The software avoids functions that enable unauthorized privilege escalations. | | DHS/DACS |
| | | **AA.2-2.** In the case of failure, the software does not grant access to unauthorized or unauthenticated users. | | OWASP Secure Coding Practices |
| **Logging (LO)** | **LO.1.** Software implements logging of all critical security incident and event information. | **LO.1-1.** Software differentiates between monitoring logs and auditing logs. | Monitoring logs record data relevant to analyzing usage and performance, troubleshooting, and informing ongoing software development. Auditing logs support analysis of and response to security events. | SAFECode "Fundamental Practices"; CWE-779 |
| | | **LO.1-2.** Software is capable of logging all security-relevant failures, errors, and exceptions. | Software development organizations should determine what information is security-relevant as part of threat-modeling (see SC.1) and risk assessment. | OWASP Secure Coding Practices; OWASP Logging Cheat Sheet; CWE-778; CWE-223 |
| | | **LO.1-3.** Software is capable of logging timestamp and identifying information associated with security incidents and events. | | SAFECode "Fundamental Practices"; OWASP Logging Cheat Sheet; CWE-778 |
| | **LO.2.** Software security incident and event information logging mechanisms are implemented securely. | **LO.2-1.** Access to logs is restricted to authorized individuals. | | OWASP Secure Coding Practices; OWASP Logging Cheat Sheet |
| | | **LO.2-2.** Logging mechanisms include anti-tamper protections. | | SAFECode "Fundamental Practices"; OWASP Logging Cheat Sheet |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE CAPABILITIES** | | | | |
| **Logging (LO)** *(continued)* | **LO.2.** Software security incident and event information logging mechanisms are implemented securely. | **LO.2-3.** Logs do not store sensitive information, such as unnecessary user information, system details, session identifiers, or passwords. | | OWASP Secure Coding Practices; OWASP Logging Cheat Sheet; CWE-532 |
| | | **LO.2-4.** Software logging mechanisms employ input validation and output encoding. | | OWASP Secure Coding Practices; OWASP Logging Cheat Sheet; CWE-117 |
| **Error and Exception Handling (EE)** | **EE.1.** Software integrates error and exception handling capabilities. | **EE.1-1.** Software identifies predictable exceptions and errors that could occur during software execution and defines how the software will handle each instance. | | DHS/DACS; OWASP Code Review Guide: Error Handling; SAFECode "Fundamental Practices"; CWE-388; CWE-390; CWE-391; CWE-396; CWE-397; CWE-544 |
| | | **EE.1-2.** Software defines how it will handle unpredicted exceptions and errors and safeguards against continued execution in an insecure state. | | DHS/DACS; OWASP Code Review Guide: Error Handling; SAFECode "Fundamental Practices"; CWE-388; CWE-390; CWE-391; CWE-396; CWE-397; CWE-544 |
| | | **EE.1-3.** Notifications of errors and exceptions do not disclose sensitive technical or human information. | | DHS/DACS; OWASP Code Review Guide: Error Handling; OWASP Secure Coding Practices; SAFECode "Fundamental Practices"; CWE-209 |
| | **EE.2.** Software fails securely; if a program is forced to terminate unexpectedly, it shuts down in a safe and responsible manner. | **EE.2-1.** Software is designed to continue operating in a degraded manner until a threshold is reached that triggers orderly, secure termination. | | DHS/DACS; CWE-636 |
| | | **EE.2-2.** In the case of failure, software reverts to secure default states that preserve confidentiality and integrity. | | CWE-636 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE LIFECYCLE** | | | | |
| **Vulnerability Management (VM)** | **VM.1.** The vendor maintains an up-to-date vulnerability management plan. | **VM.1-1.** The vulnerability management plan outlines policies, responsibilities, and expectations for both internal and external stakeholders throughout the following phases of vulnerability management: (1) the vendor's identification or receipt of a vulnerability, (2) verification of the vulnerability, (3) remediation or mitigation of the vulnerability, (4) release of a solution, and (5) post-release. | | ISO/IEC 29147; ISO/IEC 30111; SAFECode "Fundamental Practices"; SAMM |
| | | **VM.1-2.** The vulnerability management plan addresses security testing and vulnerability identification methodologies to be applied throughout a product's lifecycle. | | |
| | | **VM.1-3.** The vulnerability management plan includes a process for gaining timely awareness of and managing vulnerabilities that are discovered in third-party components of the software. | | SAFECode "Fundamental Practices"; SAMM |
| | **VM.2.** Vulnerabilities are identified and resolved rapidly and comprehensively, according to risk-based prioritization. | **VM.2-1.** Upon identification, vulnerabilities are verified and subjected to root cause and risk analysis. | | ISO/IEC 30111; SAFECode "Fundamental Practices"; SAMM |
| | | **VM.2-2.** Vulnerabilities are assigned a unique identification number. | | ISO/IEC 30111; SAFECode "Fundamental Practices" |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE LIFECYCLE** | | | | |
| **Vulnerability Management (VM)** *(continued)* | **VM.2.** Vulnerabilities are identified and resolved rapidly and comprehensively, according to risk-based prioritization. | **VM.2-3.** Vulnerabilities are assigned a severity value based on risk, using a standardized scoring methodology. | | CVSS |
| | | **VM.2-4.** Remediation and mitigation activities are informed by the severity of the vulnerability. | | ISO/IEC 30111; SAFECode "Fundamental Practices"; SAMM |
| | **VM.3.** The vendor maintains a coordinated vulnerability disclosure program. | **VM.3-1.** The vendor establishes a clearly defined and easily accessible intake mechanism to accept vulnerability information (email, portal, etc.). | | ISO 29147; SAFECode "Fundamental Practices"; SAMM; ENISA Good Practice Guide on Vulnerability Disclosure; IoT Security Foundation Vulnerability Disclosure Best Practice Guidelines |
| | | **VM.3-2.** A vendor's intake mechanism provides for secure and confidential communication of sensitive vulnerability information. | | ISO 29147; SAFECode "Fundamental Practices"; IoT Security Foundation Vulnerability Disclosure Best Practice Guidelines |
| | | **VM.3-3.** The vendor publishes, in simple and clear language, its policies for interacting with vulnerability reporters, addressing, at minimum: (1) how the vendor would like to be contacted, (2) options for secure communication, (3) expectations for communication from the vendor regarding the status of a reported vulnerability, (4) desired information regarding a potential vulnerability, (5) issues that are out of scope of the vulnerability disclosure program, (6) how submitted vulnerability reports are tracked, and (7) expectations for whether and how a reporter will be credited. | | ISO 29147; ENISA Good Practice Guide on Vulnerability Disclosure; IoT Security Foundation Vulnerability Disclosure Best Practice Guidelines |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE LIFECYCLE** | | | | |
| **Vulnerability Management (VM)** *(continued)* | **VM.3.** The vendor maintains a coordinated vulnerability disclosure program. | **VM.3-4.** The vendor maintains a system to record and track all reports of potential vulnerabilities. | | ISO 29147 |
| | | **VM.3-5.** The vendor notifies vulnerability reporters of when reported vulnerabilities are remediated or mitigated. | | ISO 29147 |
| **Configuration (CF)** | **CF.1.** The software is deployed with configurations and configuration guidance that facilitate secure installation and operation. | **CF.1-1.** The software documentation specifies configuration parameters that are as restrictive as feasible, to make sure the software is as resistant as possible to anticipated attacks and exploits. | | DHS/DACS |
| | | **CF.1-2.** The software documentation describes secure installation procedures for initial installation and installation for additional components, updates, and patches. | | BSIMM; DHS/DACS |
| | | **CF.1-3.** The software documentation describes configurations and procedures for secure configuration under normal operation. | | |
| | | **CF.1-4.** The software prompts users to change any default passwords before the software becomes operational. | | DHS/DACS |
| | | **CF.1-5.** Configuration guidance statements and configuration controls are clearly communicated and automated wherever possible. | | NIST Special Publication 800-126 |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE LIFECYCLE** | | | | |
| **Configuration (CF)** *(continued)* | **CF.1.** The software is deployed with configurations and configuration guidance that facilitate secure installation and operation. | **CF.1-6.** Software configuration settings can be altered to tailor security settings to the operating environment. | User configuration may not always be possible or necessary. However, where viable, the software should be delivered in a configuration that is as secure as possible based on its anticipated usage, and should support the ability of users to modify security settings to accommodate changing environments or requirements. | |
| **Vulnerability Notification and Patching (VN)** | **VN.1.** Vendors disseminate timely patches or updates to address identified security issues. | **VN.1-1.** Patches or updates are developed and disseminated based on risk-informed prioritization, in accordance with the vendor's vulnerability management program. | | ISO/IEC 30111; SAFECode "Fundamental Practices"; DHS/DACS; Microsoft SDL; SAMM |
| | | **VN.1-2.** Patches or updates are subjected to testing for functionality and security prior to release. | | DHS/DACS; Microsoft SDL |
| | | **VN.1-3.** All patches and updates are documented. | | DHS/DACS |
| | | **VN.1-4.** Development and dissemination of patches or updates are coordinated with other vendors where appropriate to address multi-vendor security issues or supply chain security issues. | | ISO/IEC 30111; FIRST "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure" |
| | **VN.2.** Patches or updates are disseminated securely. | **VN.2-1.** Patches or updates are transmitted in a manner that prevents exposure of the software image. | | NTIA "Voluntary Framework for Enhancing Update Process Security" |
| | | **VN.2-2.** The patch or update deliverable is cryptographically signed to ensure its integrity and authenticity. | | ISO/IEC 29147; NTIA "Voluntary Framework for Enhancing Update Process Security" |

| Category | Subcategory | Diagnostic Statement | Comments on Implementation | Relevant Standards and Informative Resources |
|---|---|---|---|---|
| **SECURE LIFECYCLE** | | | | |
| **Vulnerability Notification and Patching (VN)** *(continued)* | **VN.3.** Patches or updates for security issues are accompanied by advisory messages informing users of relevant information. | **VN.3-1.** Users are notified of a significant security issue when a remediation is in place for each supported version of the affected product. | | SAFECode "Fundamental Practices" |
| | | **VN.3-2.** Advisory messages notifying users of security issues include information on affected products, applicable versions, and platforms; a unique identification number; and a brief description of the vulnerability and its potential impact. | | ISO/IEC 29147; SAFECode "Fundamental Practices" |
| **End-of-Life (EL)** | **EL.1.** Vendor maintain consistent lifecycle guidance. | **EL.1-1.** Vendor communicates realistic assumptions and expectations regarding the nature and lifespan of product support in tandem with initial software delivery. | | |
| | | **EL.1-2.** Vendor clearly communicates decisions to terminate support for a software product to customers and users, identifying the expected support termination date; the anticipated risk of continued product use beyond the termination of support; possible mitigation actions; and options for technical migration to replacement products. | | |
| | | **EL.1-3.** Software is continually monitored to ensure that third-party components have not reached end-of-life milestones or are removed or otherwise remediated. | | |

# IV. References

## Definitions

**Access Control.** Means to ensure that access to assets is authorized and restricted based on business and security requirements. *(Source: ISO/IEC 27000: 2018)*

**Algorithm.** A finite set of well-defined rules for the solution of a problem in a finite number of steps, sequence of operations for performing a specific task, or finite ordered set of well-defined rules for the solution of a problem. *(Source: ISO/IEC/IEEE 24765: 2017)*

**Authentication.** Provision of assurance that a claimed characteristic of an entity is correct. *(Source: ISO/IEC 27000: 2018)*

**Control.** A measure that is modifying risk. Controls include any process, policy, device, practice, or other actions that modify risk. *(Source: ISO/IEC 27000: 2018)*

**Error.** Discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. *(Source: ISO/IEC 15026-1: 2019)*

**Exception.** An event that causes suspension of normal program execution, or an indication that an operation request was not performed successfully. *(Source: ISO/IEC/IEEE 24765: 2017)*

**Fault isolation.** The ability of a subsystem to prevent a fault within the subsystem from causing consequential faults in other subsystems. *(Source: ISO/IEC/IEEE 24765: 2017)*

**Fuzzing.** A means of testing that causes a software program to consume deliberately malformed data to see how the program reacts. *(Source: Microsoft Security Development Lifecycle Process Guidance Version 5.2)*

**Lifecycle.** States involved in the management of an asset; evolution of a system, product, service, project, or other human-made entity from conception through retirement. *(Sources: ISO/IEC 12207: 2017; ISO/IEC 27034: 2011)*

**Mitigation.** The process of remediating a weakness, leaving the software in a more secure state. *(Source: Common Weakness Enumeration/MITRE)*

**Patch.** A modification made directly to an object program without reassembling or recompiling from the source program, or a software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. *(Source: ISO/IEC 19770-2: 2015)*

**Penetration testing.** A test method in which the security of a computer program or network is subjected to deliberate simulated attack. *(Source: Microsoft Security Development Lifecycle Process Guidance Version 5.2)*

**Release gate.** A specific point established in the software development lifecycle where a project may not move forward until it meets certain security conditions established by an organization at the project's inception. *(Adapted from Software Assurance Maturity Model, Version 1.0)*

**Risk.** 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. *(Source: BSA International Cybersecurity Policy Framework)*

**Sandboxing.** A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. *(Source: Committee on National Security Systems No. 4009)*

**Software.** All or part of the programs that process or support the processing of digital information. *(Source: ISO/IEC 12207: 2017)*

**Third-party components.** Components of a software project of external origin, including open-source components, purchased commercial off-the-shelf software, and online services used by the software project. *(Adapted from Software Assurance Maturity Model, Version 1.5)*

**Threat modeling.** A systematic exploration technique to expose any circumstance or event having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service. *(Source: ISO/IEC/IEEE 24765: 2017)*

**Vulnerability.** Weakness of software, hardware, or online service that can be exploited. *(Source: ISO/IEC 30111: 2013)*

**Weakness.** A type of mistake in software that, in proper conditions, could contribute to the introduction of vulnerabilities within that software. *(Source: Common Weakness Enumeration/MITRE)*

## Acronyms

| | |
|---|---|
| **BSIMM** | Building Security in Maturity Model, Version 9 |
| **CAPEC** | Common Attack Pattern Enumeration and Classification |
| **CVSS** | Common Vulnerability Scoring System |
| **CWSS** | Common Weakness Scoring System |
| **DHS/DACS** | Department of Homeland Security/Data & Analysis Center for Software, *Enhancing the Development Life Cycle to Produce Secure Software*, Version. 2.0. |
| **DoD-PPP** | Department of Defense, "Software Assurance Countermeasures in Program Protection Planning" |
| **FIPS** | Federal Information Processing Standards |
| **ISO/IEC** | International Organization for Standardization/International Electrotechnical Commission |
| **Microsoft SDL** | Microsoft's Security Development Lifecycle Process Guidance, Version 5.2 |
| **NCSC** | United Kingdom National Cyber Security Centre Secure Development and Deployment Guidance |
| **NIST** | National Institute for Standards and Technology |
| **NIST IR** | NIST Interagency Report |
| **NIST SP** | NIST Special Publication |
| **NTIA** | National Telecommunications and Information Administration |
| **NVD** | National Vulnerability Database |
| **OAuth** | Initiative for Open Authentication |
| **OIDC** | OpenID Connect |
| **OWASP** | Open Web Application Security Project |
| **SAFECode "Fundamental Practices"** | SAFECode *Fundamental Practices for Secure Software Development*, Version 3.0 |
| **SAML** | Security Assertion Markup Language |
| **SAMM** | Software Assurance Maturity Model, Version 1.5 |
| **SEI** | Carnegie Mellon University's Software Engineering Institute |
| **SPDX** | Software Package Data Exchange, Version 2.1 |
| **U2F** | Universal Second Factor |
| **UAF** | Universal Authentication Framework |
| **WS-FED** | Web Services Federation Language, Version 1.2 |

## Sources


Adobe, Adobe Secure Engineering Overview, March 2018. https://www.adobe.com/content/dam/acom/en/security/pdfs/adobe-secure-engineering-wp.pdf.

Apple, *Secure Coding Guide*. https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html.

Box, *Box Platform Guidelines and Security*. https://developer.box.com/docs/security-guidelines.

BSA | The Software Alliance, *BSA International Cybersecurity Policy Framework*. https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf.

Carnegie Mellon University Software Engineering Institute, *SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems*, 2016 Edition, June 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=454220.

Carnegie Mellon University Software Engineering Institute, *SEI CERT C++ Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems*, 2016 Edition, March 2017. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=494932.

Carnegie Mellon University Software Engineering Institute, *SEI CERT Oracle Coding Standard for Java*, October 11, 2016. https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java.

Committee on National Security Systems (CNSS), *Committee on National Security Systems Glossary*, CNSS Instruction No. 4009, April 6, 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

European Union Agency for Network and Information Security, *Good Practice Guide on Vulnerability Disclosure*, January 18, 2016. https://www.enisa.europa.eu/publications/vulnerability-disclosure.

FIDO Alliance, *Universal 2nd Factor Overview*, April 11, 2017. https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf.

FIDO Alliance, *Universal Authentication Framework Architectural Overview*, Version 1.1, February 2, 2017. https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.html.

Forum for Incident Response and Security Teams, *Common Vulnerability Scoring System: Specification Document*, Version 3.0. https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf.

Forum for Incident Response and Security Teams, *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure*, Version 1.0, Summer 2017. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-latest.pdf?20180320.

Howard, Michael and Steve Lipner, *The Security Development Lifecycle: A Process for Developing Demonstrably More Secure Software*, 2006, Redmond, WA: Microsoft Press.

IBM, *Security in Development: The IBM Secure Engineering Framework*, 2010. https://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf.

Initiative for Open Authentication, *OAuth 2.0*, October 2012. https://oauth.net/2/.

International Organization of Standardization, *Information Technology—IT Asset Management—Parts 1–2*, ISO/IEC 19770 (1: 2017–2: 2015).

International Organization of Standardization, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, ISO/ IEC 27000: 2018.

International Organization of Standardization, *Information Technology—Security Techniques—Entity Authentication—Parts 1–3*, ISO/IEC 9798- (1: 2010–3: 2019).

International Organization of Standardization, *Information Technology—Programming Languages, Their Environments and System Software Interfaces—C Secure Coding Rules*, ISO/IEC TS 17961: 2013.

International Organization of Standardization, *Information Technology—Security Techniques—Encryption Algorithms—Parts 1–5*, ISO/IEC 18033 (1: 2015–5: 2015).

International Organization of Standardization, *Information Technology—Security Techniques—Authenticated Encryption*, ISO/IEC 19772: 2009.

International Organization of Standardization, *Information Technology—Security Techniques—Security Requirements for Cryptographic Modules*, ISO/IEC 19790: 2012.

International Organization of Standardization, *Information Technology—Security Techniques—Application Security; Parts 1–7*, ISO/IEC 27034 (1:2011–7:2018).

International Organization of Standardization, *Information Technology—Security Techniques—Vulnerability Disclosure*, ISO/IEC 29147: 2018, October 23, 2018.

International Organization of Standardization, *Information Technology—Security Techniques—Vulnerability Handling Processes*, ISO/IEC 30111: 2013(E), November 1, 2013.

International Organization of Standardization, *Systems and Software Engineering—Software Lifecycle Processes*, ISO/IEC/IEEE 12207: 2017.

International Organization of Standardization, *Systems and Software Engineering—Systems and Software Assurance—Part 1: Concepts and Vocabulary*, ISO/IEC/IEEE 15026 (1: 2019).

International Organization of Standardization, *Systems and Software Engineering—Vocabulary*, ISO/IEC/IEEE 24765: 2017.

IoT Security Foundation, *Vulnerability Disclosure: Best Practice Guidelines, Release 1.1*, December 2017. https://iotsecurityfoundation.org/wp-content/uploads/2017/01/Vulnerability-Disclosure.pdf.

The Linux Foundation, Software Package Data Exchange, Specification Version 2.1, 2016. https://spdx.org/sites/cpstandard/files/pages/files/spdxversion2.1.pdf.

McGraw, Gary, Sammy Migues, and Jacob West, *Building Security in Maturity Model (BSIMM)*, Version 9, 2018. https://www.bsimm.com.

Microsoft, *Security Development Lifecycle: SDL Process Guidance*, Version 5.2, May 23, 2012. https://www.microsoft.com/en-us/download/details.aspx?id=29884.

MITRE Corporation, *Common Attack Pattern Enumeration and Classification*, Version 3.0. https://capec.mitre.org/data/index.html.

MITRE Corporation, Common Weakness Enumeration, Version 3.2. https://cwe.mitre.org/data/index.html.

MITRE Corporation, *Common Weakness Scoring System*, Version 1.0.1, September 5, 2014. https://cwe.mitre.org/cwss/cwss_v1.0.1.html.

MITRE Corporation and the SANS Institute, *CWE/SANS Top 25 Most Dangerous Software Errors*, Version 1.0.3, September 13, 2011. https://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.pdf.

OASIS, *Security Assertion Markup Language*, Version 2.0, March 25, 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf.

OASIS, *Web Services Federation Language*, Version 1.2, May 22, 2009. http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html.

Okta, *Okta Security Technical White Paper*. https://www.okta.com/sites/default/files/Okta%20Technical%20Security%20Whitepaper.pdf.

Open ID Foundation, *Open ID Connect*, Version 1.0, November 8, 2014. https://openid.net/connect/.

Open Web Application Security Project (OWASP), *Application Security Verification Standard*, Version 3.0, October 2015. https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf.

Oracle, *Security Practices: Oracle Software Security Assurance*. https://www.oracle.com/corporate/security-practices/assurance/.

OWASP, *Attack Surface Analysis Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.md.

OWASP, *Authentication Cheat Shee*t. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Authentication_Cheat_Sheet.md.

OWASP, *C-Based Toolchain Hardening Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/C-Based_Toolchain_Hardening_Cheat_Sheet.md.

OWASP, *Code Review Guide*, Version 2.0, July 2017. https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf.

OWASP, *Cryptographic Storage Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cryptographic_Storage_Cheat_Sheet.md.

OWASP, *Development Guide*, Version 2.0.1, June 2014. https://github.com/OWASP/DevGuide/tree/dc5a2977a4797d9b98486417a5527b9f15d8a251/DevGuide2.0.1.

OWASP, *Input Validation Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md.

OWASP, *Logging Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Logging_Cheat_Sheet.md.

OWASP, *OWASP Top 10 — 2017: The Ten Most Critical Web Application Security Risks*, 2017. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

OWASP, *Password Storage Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Password_Storage_Cheat_Sheet.md.

OWASP, *Secure Coding Practices Quick Reference Guide*, Version 2.0, November 2010. https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf.

OWASP, *Software Assurance Maturity Model*, Version 1.5, April 2017. https://owaspsamm.org/v1-5/downloads/.

OWASP, *Testing Guide*, Version 4.0, September 2014. https://www.owasp.org/images/1/19/OTGv4.pdf.

OWASP, *Threat Modeling Cheat Sheet*. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Threat_Modeling_Cheat_Sheet.md.

SAFECode, *Fundamental Practices for Secure Software Development*, Third Edition, March 2018. https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

SAFECode, *Fundamental Practices for Secure Software Development*, Second Edition, February 2011. https://safecode.org/publication/SAFECode_Dev_Practices0211.pdf.

SAFECode, *Managing Security Risks Inherent in the Use of Third-Party Components*, 2017. https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf.

SAFECode, *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*, July 21, 2009. http://safecode.org/publication/SAFECode_Supply_Chain0709.pdf.

SAFECode, *Tactical Threat Modeling*, May 2017. https://safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf.

Salesforce, *Secure Coding Guide*, Version 45.0, January 30, 2019. https://resources.docs.salesforce.com/218/latest/en-us/sfdc/pdf/secure_coding.pdf.

Symantec, "Executive Summary: Symantec Software Security Process," 2019. https://www.symantec.com/content/dam/symantec/docs/other-resources/symantec_software_security_process.pdf.

United Kingdom National Cyber Security Centre Secure, *Guidance for Secure Development and Deployment*, December 11, 2017. https://www.ncsc.gov.uk/guidance/secure-development-and-deployment.

United States Department of Defense, "Software Assurance Countermeasures in Program Protection Planning," March 2014. https://www.acq.osd.mil/se/docs/swa-cm-in-ppp.pdf.

United States Department of Homeland Security/ Data & Analysis Center for Software, *Enhancing the Development Life Cycle to Produce Secure Software*, Version. 2.0, October 2008. http://www.seas.upenn.edu/~lee/09cis480/papers/DACS-358844.pdf.

United States National Institute for Standards and Technology, *BIOS Protection Guidelines: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-147, April 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf.

United States National Institute for Standards and Technology, *Digital Identity Guidelines, Special Publication 800-63-3*, June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

United States National Institute for Standards and Technology, *Federal Information Processing Standards*. https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips.

United States National Institute for Standards and Technology, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags, Interagency Report 8060*, April 2016. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf.

United States National Institute for Standards and Technology, *National Vulnerability Database*. https://nvd.nist.gov/.

United States National Institute for Standards and Technology, *Notional Supply Chain Risk Management Practices for Federal Information Systems, Interagency Report 7622*, October 2012. https://csrc.nist.gov/publications/detail/nistir/7622/final.

United States National Institute for Standards and Technology, *Recommendation for Key Management: Part I: General, Special Publication 800-57*, Revision 4, January 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.

United States National Institute for Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53*, Revision 4, April 2013. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.

United States National Institute for Standards and Technology, *The Technical Specification for the Security Content Automation Protocol, Special Publication 800-126*, Revision 3, February 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf.

United States National Telecommunications and Information Administration, *Voluntary Framework for Enhancing Update Process Security*, October 31, 2017. https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf.


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

## Annex C

# BSA Principles for Good Governance: Supply Chain Risk Management

# BSA Principles for Good Governance: Supply Chain Risk Management

*Managing security risks to information technology supply chains is an important priority for both governments and businesses globally. Information and communications technologies store, process, and transmit vast volumes of data, underpin the global digital economy and support the operations of governments, critical infrastructures, and societies. When malicious actors exploit supply chain vulnerabilities, they can cause unacceptable harm to privacy, security, and commerce. Yet, mistargeted policy interventions aimed at improving security can introduce unintended consequences by causing severe damage to the technologies and economic activities they seek to protect.*

*Effective government approaches to supply chain risk management recognize the global, interconnected nature of supply chains and the threats against them, identifying and disrupting malicious actors through policies and processes that are sustainable, reciprocal, and transparent.*

*As governments around the world seek to address supply chain risk management, BSA asserts the principles below to guide effective policy responses. BSA will use these principles to evaluate national supply chain risk management policies and to work toward enhancing the security, integrity, and vitality of the global digital economy.*

## Risk Management

Governments should adopt risk management approaches to supply chain security. Risk management entails understanding risk through the identification of likely threats, vulnerabilities and potential consequences, tailoring mitigation strategies to risks, and prioritizing actions based on the most relevant and potentially impactful risks. Risk management approaches retain flexibility that enable security practitioners within both governments and businesses to adapt to a constantly evolving threat environment. Finally, risk management approaches consider not only risks from malicious actors, but also the risks, timelines, and costs associated with potential mitigation options, helping policymakers avoid unintended consequences of mistargeted policies.

A corollary to this principle is that supply chain security policies should empower governments to take action based on security risks. Further, policies should foster, not hinder, global technology competition, and allow nations to meet their international trade commitments.

## Interoperability

Modern technology supply chains are often transnational, and so too are threats against them. As such, effective policies will embrace interoperability – consistency and compatibility of regulations and technical standards across national borders – and will avoid adopting categorical prohibitions against the acquisition or integration of technologies simply because they are developed abroad. A good rule of thumb is: a government should adopt policies only to the extent it is comfortable with other governments enforcing those policies against its own businesses.

Building policies around internationally recognized, industry driven standards ensures that technology providers can develop, maintain, and secure innovative products across global boundaries and help to facilitate transnational operational collaboration against significant cyber threats.

## Transparency

Opaque government supply chain risk management policies and processes, such as the debarment of certain foreign vendors from acquisition processes without notification or justification, create confusion and can prompt protectionist interventions by other governments, undermining the economic competitiveness of global businesses. Absent exceptional circumstances, government supply chain risk management policies and their implementation should be transparent to the public, with specific actions notified to impacted stakeholders. In any case in which a government denies market access to a vendor or technology, that government should articulate a public justification outlining specific security concerns prompting the action.

In addition, the transparency principle should oblige the government to provide for disclosure of identified supply chain vulnerabilities to suppliers, in accordance with vulnerability disclosure methodologies described in ISO/IEC 29147. Government vulnerability disclosure can improve the overall security of the digital ecosystem and improve public-private collaboration against supply chain threats.

## Discretion

Enhancing supply chain security means, in part, developing a more secure global cybersecurity ecosystem that recognizes norms for responsible behavior and prioritizes collective defense against malicious threats. Governments should pledge that they will not undertake systemic interventions in global supply chains.

## Enforcement

While state actors may present the most sophisticated threats, supply chains are also under constant pressure from non-state actors engaging in malicious cybersecurity activity, counterfeiting, product diversion, and related activities. A key element of a government's supply chain risk management strategy must be to pursue aggressive law enforcement against malicious actors within its jurisdiction.

## Collaboration

Government supply chain risk management efforts will be most effective when undertaken in collaboration with key non-governmental stakeholders, including industry. As industry increasingly provides leadership on addressing supply chain concerns, governments should embrace creative opportunities for public-private partnerships aimed at securing supply chains and developing best practices for supply chain risk management. Recent efforts like the Paris Call for Trust and Security in Cyberspace are promising. Likewise, collaboration should be sought on a government-to-government basis with key partners through the expansion of supply chain threat information-sharing and operational cooperation against supply chain threats.

## Fairness

Supply chain risk management processes should establish meaningful mechanisms for resolving disputes, including opportunities for impacted stakeholders to appeal or protest decisions, provide defense against any alleged offenses, and remediate past concerns. Dispute resolution mechanisms create an environment of certainty and predictability without limiting tools for mitigating risk.

## Research and Development

Securing global supply chains will be an ongoing challenge – one in which security techniques must adapt to an ever-changing environment of new technologies and new threats. By investing in the research and development of new technological approaches to fostering supply chain integrity, governments can gain and maintain the advantage against malicious actors. Promising areas of research include the use of blockchain-based technologies, development of processes to vet third-party components for security issues, and the application of artificial intelligence for the analysis of supply chain data and anomaly detection, among others.