CISA GLOBAL

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

FEBRUARY 2021

Message FROM THE Director

There are moments in the history of our Nation when Congress and the President deem it necessary to create a new executive agency to serve the American people. The establishment of the Department of Homeland Security (DHS) itself was one of these moments. Sixteen years later, in November 2018, we recognized that there must be a single organization to lead the national effort to protect our critical infrastructure. Today, that agency is the Cybersecurity and Infrastructure Security Agency (CISA), "the Nation's Risk Advisor."

CISA achieves its core mission of leading cybersecurity and infrastructure security programs, operations, and policy through its key mission areas: cybersecurity, infrastructure security, and emergency communications. As threats to these missions are increasingly global and interconnected, the solutions we pursue to address these risks must often reflect a world-wide approach.

Cybersecurity has become a core component of homeland security. CISA carries out its cybersecurity mission by: (1) leading Federal Government efforts to secure networks of federal civilian executive agencies; (2) working with the public, private sector, and international partners to enhance critical infrastructure cybersecurity and resilience; (3) responding to significant cyber incidents; and (4) strengthening the security, privacy, and reliability of the global cyber ecosystem.

Promoting robust international collaboration is instrumental to accomplishing the Department's cybersecurity objectives as threats in cyberspace are not constrained by borders. Similarly, U.S. critical infrastructure is increasingly interconnected and dependent on global infrastructure, supply chain, and systems whose cybersecurity practices and maturity can vary widely. Emergency communications mechanisms also have an international nexus, with U.S. systems including and depending on elements and arrangements that cross our borders. Therefore, other nations and international organizations are key partners across our efforts. Appropriately and securely sharing threat information, mitigation advice, and best practices with international partners not only reinforces good cyber hygiene, but also bolsters the resiliency within our respective systems and critical infrastructure, which in turn, foster a safer cyber-physical ecosystem for all.

As CISA strives to expand its global partnerships, we must ensure that our international engagement and related operations reflect broader U.S. national security, economic, and foreign policy goals to effectively identify and implement our cyber and infrastructure security objectives. To achieve this, our priority international efforts will focus on executing and advancing the CISA Director's operational priorities that span across CISA's goals and objectives.

CISA Global outlines our approach to how CISA will work with international partners to fulfill our responsibilities, execute our work, and create unity of effort within our mission areas. This strategy presents the global vision and international operational priorities of the CISA Director, consistent with CISA's international authorities as outlined in the Homeland Security Act of 2002; Department of Homeland Security's Strategic Plan for FY 2020-2024; EO 13800 Report, DHS International Cybersecurity Priorities; and the CISA Strategic Intent. This overarching strategy provides an approach for how CISA will execute its responsibilities and serves as a reference point to guide our work and create unity of effort.

Brandon Wales
Acting Director

CISA AT A GLANCE

WHO WE ARE

CISA works with partners across government and industry to defend against today's threats and collaborates to build more secure and resilient infrastructure for the future.

- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS
- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE

DIRECTOR'S OPERATIONAL PRIORITIES

The Director has five specific operational areas of focus that, in some cases, span across several goals and objectives.

1. CHINA, SUPPLY CHAIN, AND 5G
2. ELECTION SECURITY
3. SOFT TARGET SECURITY
4. FEDERAL CYBERSECURITY
5. INDUSTRIAL CONTROL SYSTEMS

WE ARE THE NATION'S RISK ADVISOR

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.

A GLOBAL VISION

MISSION

Enhance our national security and resilience by working with international partners to strengthen the security of the cyber ecosystem; increase the resiliency of critical infrastructure; and address urgent threats and manage risks that are critical to U.S. interests.

VISION

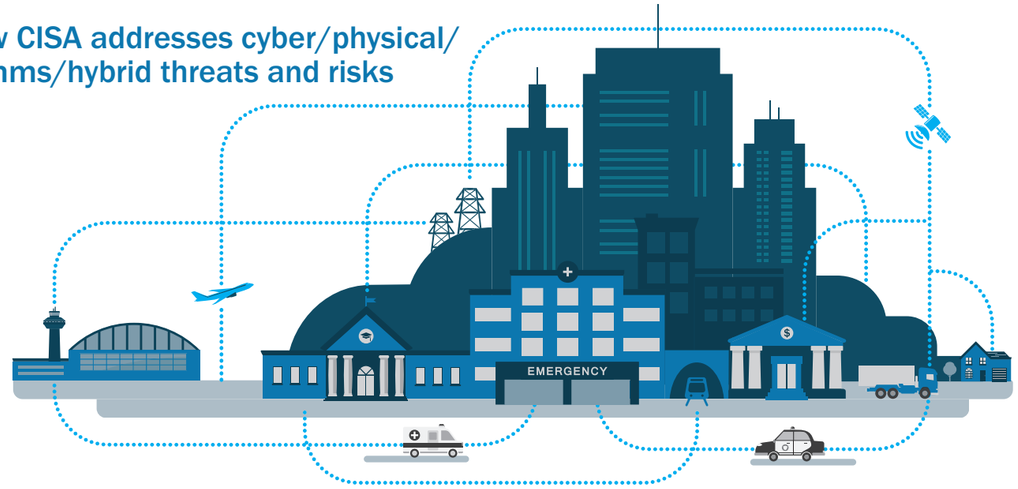
A more open, interoperable, reliable, and secure interconnected world that fosters a global operational and policy environment where government and industry security professionals and risk managers can collectively stop threats and address risks to critical infrastructure while engaging with stakeholders and building capacity. CISA seeks to promote best practices in security and resilience measures across all critical infrastructure sectors and to promote global communications infrastructure assets and systems, including internet connectivity that is open, interoperable, reliable, and secure.

In today's globally and interconnected world, we confront a wide array of serious risks and threats to our critical infrastructure, systems, assets, functions, and citizens. State and non-state actor adversaries and competitors seek to advance their objectives through a variety of tactics, including subtle actions that significantly weaken the foundations of U.S. power, degrade societal functions, undermine trust in institutions, and increase adversaries' ability to exploit vulnerabilities and undermine the functions of critical infrastructure. Extreme weather events, natural hazards, terrorism, and hostile state actors are among the threats to critical functions, the "systems of systems," and systemic risks that can have global, cascading effects.

As networked devices are further integrated into lives and businesses, their vulnerabilities provide additional attack vectors for nation-states and foreign adversaries. For example, global supply chains face risks from malicious activity to software and hardware, disruptions from physical attacks or natural events, and manipulation for political and economic purposes; aging, outdated, and under-resourced infrastructures may not sustain a confrontation to the system; emergency communication between first responders and decision-makers may be at risk from disruption or lack of interoperability and localized incidents may create a shortage of items that are critical dependencies for partner nations. Many of these risks are complex — and are dispersed both geographically and across a variety of stakeholders.

CISA is uniquely equipped to serve as the central coordinator for information sharing, analysis, planning, and response, while working in concert with like-minded international partners. As the national Computer Security Incident Response Team (CSIRT) of the U.S. Government — sometimes colloquially referred to as the national Computer Emergency Readiness or Response Team (CERT).CISA works alongside the global community of CSIRTs to serve as the "first responders of the cyber world." As part of this community, CISA leverages its network and partnerships to enhance the security and resilience of global cybersecurity which helps protect foreign partners, the private sector, and individuals from hostile actors by sharing information, exchanging best practices, and heightening awareness among our stakeholders and the general public.

How CISA addresses cyber/physical/ comms/hybrid threats and risks



Furthermore, in today's interdependent and interconnected world, the safety and security of critical infrastructure requires the concerted efforts of public and private partners around the globe. CISA's focus on infrastructure security includes addressing bombing security, chemical security, soft target security, and insider threat mitigation. Consistent with CISA's statutory authorities, CISA collaborates with international partners to enhance and promote cross-border and global critical infrastructure security and resilience through information sharing so we can all benefit from the exchange of best practices, expertise, and lessons learned.

With these critical mission sets, CISA must do more to address today's complex challenges and to prepare for future threats. CISA can leverage its global network to strengthen partner capacity and to build a better, collective practice posture and response to urgent threats that are particularly critical to U.S. national security interests.

CISA is committed to promoting an open, interoperable, reliable and secure interconnected world within a global, operational and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical infrastructure. We invite our global partners to join us in the fight to secure today and to defend tomorrow.

WHAT IS A CSIRT?

CISA also has a unique role in engaging with the global community of Computer Security Incident Response Teams (CSIRT) and is the national CSIRT of the U.S. Government. A CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility of providing incident management capability for an organization. When a CSIRT exists in an organization, it is generally the focal point for coordinating and supporting incident response.

DHS has regular engagement with national-level CSIRTs. A "CSIRT with national responsibility" is that which has been designated by a country or economy to have specific responsibilities in cyber protection or incident response, usually to support national security goals and address government networks and/or critical infrastructure. National CSIRTs must be specifically recognized as such by the government for which they operate.

CSIRTs serve as the "first responders" of the cyber world, protecting governments, companies, and individuals from attackers, sharing best practices, and improving awareness among their cybersecurity counterparts, governments, the private sector, and the general public. Historically, this technical community focused on network protection or computer network defense and relied on a culture of technical cooperation in any circumstance. This has enabled CSIRTs to cooperate regardless of political issues and maintain a singular focus on incident response and mitigation.

CISA'S VISION FOR INTERNATIONAL PARTNERS

CISA protects U.S. critical infrastructure from today's threats, while also focusing on tomorrow's emerging risks. As the national lead for protecting and enhancing the security and resilience of the Nation's federal civilian cyber systems and critical infrastructure, CISA adopts a risk management approach that reduces systemic vulnerabilities across the Nation to collectively increase our protective and defensive posture against malicious cyber activity, hybrid threats, terrorism and targeted violence, and the full range of infrastructure security risks. CISA works with public and private sector entities to ensure owners, operators, and stakeholders are informed and well-equipped to make risk management decisions about their systems and assets.

DHS and CISA's international priorities are driven by its unique homeland security mission. International partnerships are therefore best seen as a fundamental element of mission execution for components with cybersecurity and critical infrastructure responsibilities. In this context, CISA would like to build, sustain, and advance international partnerships to:

- Strategically cultivate international support for CISA's objectives, priorities, and core functions, as well as broader DHS and U.S. national security goals;
- Increase awareness of – and guide global strategic communication – on vulnerabilities and risks to cybersecurity, infrastructure security, and emergency communications;
- Facilitate information sharing to help prevent, mitigate, and manage cyber and physical risks to enhance the security and resiliency of critical infrastructure; supply chains; and the global cyber ecosystem;
- Bolster operational capacity and address identified capability gaps and technological and information requirements;
- Share expertise and best practices to build and strengthen network protection, risk management, and incident response capacity;
- Manage systemic risks to help maintain international stability; and
- Broadly shape the evolving cyber ecosystem to support its overall cybersecurity mission.

LINES OF EFFORT

CISA will focus its engagement with the global community through four lines of effort that both coincide with our approach to international partnerships and align with broader strategic goals: (1) operational cooperation; (2) capacity building; (3) stakeholder engagement and outreach; and (4) shaping the policy environment. Core to each of these lines of effort is information sharing.

Appropriate and secured information sharing is a critical part of CISA's international collaborative activities. CISA utilizes key programs, such as Automated Indicator Sharing (AIS) and the Homeland Security Information Network (HSIN), to amplify our relationships. These programs help the United States and its allies protect against, identify, warn of, and respond to threats and incidents; leverage information that builds capacity of critical infrastructure owners and operators in both the public and private sectors; and maintain and secure a functioning, resilient infrastructure that is crucial to bolstering public confidence and national/economic security.

— INFORMATION SHARING —

OPERATIONAL COOPERATION

CAPACITY BUILDING

STAKEHOLDER ENGAGEMENT & OUTREACH

SHAPING THE POLICY ECOSYSTEM

OPERATIONAL COOPERATION

Given the increasing interconnectedness of our networks, the interdependencies among critical infrastructure sectors, and cross-border data flows, operational cooperation with foreign counterparts is a key tool in collaborating to prevent, detect, deter, and mitigate threats and hazards effectively. Operational cooperation, for the purposes of this document, can be defined as engagement with international partners that is characterized by mutually beneficial information sharing that informs and enhances our relationships. Through such international operational cooperation, CISA can improve its collective situational awareness, and is able foster innovative approaches for responding to and mitigating threats and hazards to critical infrastructure and cybersecurity. Developing CISA's partnerships into trusted relationships will enable critical operational information sharing that can improve communications capabilities, foster an environment for joint operations, and support resilience efforts – whether that be by sharing operational best practices, working on joint exercises, addressing threat information and related mitigation advice, or collaborating in a fashion so as to align security and defense efforts with like-minded partners. Ultimately, CISA seeks to mature our partnerships to establish an attaché program and to deploy personnel overseas to effectively execute CISA's mission.

GOAL 1: INCREASE SITUATIONAL AWARENESS

Advance CISA's ability to maintain continuous situational awareness of physical and cyber incidents and emergency communications issues and to identify concerns and threats that may impact critical infrastructure in order to facilitate an expedited response and mitigate negative consequences.

STRATEGIC OBJECTIVE

Public and private owners and operators manage the vast array of critical infrastructure supporting the U.S. economy and communities. These systems and assets provide national critical functions that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on the Nation's security, economy, and public health and safety. Infrastructure systems are rapidly evolving to capitalize on new technology and opportunities to enhance their services, and adversaries are constantly evolving to outpace stove-piped defenses. Increasingly, infrastructure owners and operators worldwide face new risks and must address nation-state adversarial actions. Serving as the lead for critical infrastructure security and cybersecurity across the Federal Civilian U.S. Government, CISA promotes the adoption of common policies and best practices that are risk-based and responsive to the ever-changing threat environment. Additionally, as lead for national cybersecurity asset response, we collaborate with interagency counterparts to deploy capabilities for intrusion detection, unauthorized access prevention, and near real-time cybersecurity risk reports. In deploying these capabilities, CISA prioritizes assessments, security measures, and remediation for systems that could significantly compromise national security, foreign relations, the economy, public confidence, or public health and safety.

DESIRED OUTCOMES

- Bolster the security of global critical infrastructure by understanding evolving risks, prioritizing risk management activities to better secure infrastructure, and taking actions to respond to emerging threats, with an emphasis on improving defense of cyber threats and cyber asset response.
- Secure civilian information technology systems globally from cyber threats and intrusions while working with likeminded partners.

Objective 1: Assess and Counter Evolving Risks

1. Build, sustain, and advance international relationships to (1) prevent incidents, protect infrastructure, mitigate, and manage risks and (2) enhance the security and resiliency of the global cyber ecosystem, and protect privacy.
2. Enhance CISA's understanding of the threat activity and strategic interests of major threats and obtain timely access to available data on the risk posture of key information systems and other critical infrastructure.
3. Increase CISA's ability to analyze and prioritize risk and prevent or mitigate significant threat activity and vulnerabilities through prevention, protection, and response actions.
4. Advise and share threat indicators and other information with international partners, as appropriate.
5. Utilize CISA's authorities, and leverage those of DHS and the U.S. interagency, to effectively and efficiently combat threats by exchanging actionable, relevant, and timely threat intelligence with international partners.
6. Maintain awareness of trends in international and systemic cybersecurity and infrastructure risks, including those impacting global information and communication technology supply chains, and other systemic risks that affect national security, public health and safety, and economic security.
7. Develop strategies and actionable solutions to respond to emerging risks in collaboration with relevant international partners.
8. Promote use of similar mechanisms of communications used by emergency responders and government officials with like-minded partners to ensure we remain safe, secure, and resilient.
9. Convene government, private sector, and international partners to advance best practices and collective defenses that promote security and resilience across the United States' expansive critical infrastructure and the larger global cyber ecosystem.
10. Leverage feedback from international partners to plan more strategically to match and surpass the pace and innovation of adversaries as CISA leverages its national risk management approach to jointly assess cyber risks, develop plans for specific threats, and implement tailored solutions to protect our critical assets

DESIRED OUTCOMES

- Work with international partners and participate as members of the international security community and with critical infrastructure and industrial control system owners and operators within their national systems to ensure a safe and secure global environment while mitigating threats that we face collectively.

Objective 2: Strengthen the Security and Resilience of U.S. Critical Infrastructure.

1. Work with international partners, as well as the private and public sectors, to minimize the impacts of physical hazards through coordinated preparedness activities to enhance the security and resiliency of U.S. critical infrastructure and, in turn, help international partners prepare for, respond to, and recover from physical hazards to their critical infrastructure.
2. Augment CISA's understanding of imminent threats and ability to prepare for and respond to incidents involving natural hazards; special events; and mass gatherings by sharing best practices and lessons learned with international partners.all threats and hazards.
3. Enhance the security and resilience of U.S. critical infrastructure and overseas assets of interest to the United States (particularly in countries that border the United States with whom we share critical infrastructure) through sharing information, risk management approaches, best practices, and training information.
4. Assess cross-sector critical infrastructure risks and global interdependencies and provide expertise and services to critical infrastructure stakeholders in the United States and abroad.
5. Support owners and operators of critical infrastructure overseas that impacts U.S. national and economic security by performing vulnerability and risk assessments, promoting the research and development of security technologies, and providing other technical services to improve the security and resilience of that critical infrastructure against threats and hazards.
6. Reduce risk to U.S. critical infrastructure by working with international partners to strengthen Industrial Control Systems' (ICS) security and resilience.
7. Leverage interagency work for a common understanding of strategic threats – and best practices in securing critical infrastructure against them – that can empower international partners, private sector security professionals, critical infrastructure owners and operators, and government partners to improve resilience and integrity of critical functions within the global sphere.

CAPACITY BUILDING

GOAL 2: BUILD PARTNER CAPACITY

Liaise with and support international partners in developing their own capacity to effectively detect threats, assess impact potential, and take appropriate response actions to mitigate risk that enable cooperation with and increase benefits for CISA divisions.

The global implications of all threats and hazards — especially those stemming from the cyber-physical nexus — actuates CISA to assist countries in building their own competency in managing risk, strengthen security and resilience, and address current and emerging risks. Enhancing other countries' organic capabilities simultaneously enables CISA to comprehensively protect the Homeland, to bolster international security, and to promote global societal resilience. Sharing lessons learned, best practices, and information sharing while leveraging the technology, research, and capacities of other nations will be the cornerstone of this effort while working with Department of State.

STRATEGIC OBJECTIVE

Increasing global security and resilience capacity, including cybersecurity due diligence, as well as the development and maturation of CSIRTs is necessary to address current and evolving cybersecurity risks. DHS and other agencies have committed significant resources to supporting such efforts over the years. Long-term benefits from investment in cybersecurity and infrastructure capacity building are often not fully realized because of political shifts in recipient countries, the lack of good mechanisms for follow up, or a lack of incentives for trained individuals to remain in their jobs. CISA would like to work with international partners to explore ways to prioritize and sustain investments in capacity building such as providing more readily accessible resources for cybersecurity capacity building overall.

DESIRED OUTCOMES

- Increased number of foreign counterparts with the capacity to connect to CISA critical information sharing systems, and vice-versa. This includes enhancing coordination and operational tempos with prioritized partnerships to share real time threat information during steady state and emergency operations.
- Strengthened security and resilience for overseas infrastructure of critical importance to the United States.
- Increased awareness, identification, and early warning of those wishing to cause harm to the United States and our foreign partners.
- Increased capabilities of CISA elements following the incorporation and adaptation of best practices and lessons identified from foreign counterparts.

Objective 1: Increase Partner Capacity and Awareness

1. Enhance and support bilateral, regional and global initiatives to improve nations' capabilities in the areas of cybersecurity, critical infrastructure protection, and physical security. Partner with governments, industry, and civil society to build global cybersecurity and critical infrastructure security capacity.
2. Enhance national security domestically and globally by exchanging critical infrastructure security and resilience materials, best practices, and lessons identified and learned with select international partners on key issues of mutual interest.
3. Contribute CISA's expertise to assist countries to develop their own capacity, in turn protecting the Homeland and assets abroad while effectively enabling CISA to learn from countries with expertise on specific areas of interest.
4. Drive the development of international policies and standards on emergency communications governance and capacity building to improve interoperability so that responders have the ability to seamlessly share voice, video, and data communications during daily operations; major incidents; events.
5. Encourage increased numbers of cyber and physical security-trained professionals to ensure that there is an appropriate supply to meet international demand.

STAKEHOLDER ENGAGEMENT & OUTREACH

GOAL 3: STRENGTHEN COLLABORATION

Strengthen collaboration with foreign counterparts to enable a common understanding of threats and hazards and increase preparedness for the shared responsibility of protecting vital infrastructure and information systems.

The CISA international mission depends upon strategic stakeholder engagement to establish a vast, diverse, and robust network of public and private stakeholders and experts in order to promote a collective effort towards protecting critical infrastructure and strengthening the global cyber posture. CISA aims to build and to mature partnerships internationally to create channels of communication that facilitate the exchange of information, best practices, ideas, and lessons-learned as well as to remain timely and relevant on ongoing global efforts to address common issues. Through stakeholder engagement and outreach, CISA is not only able to raise awareness to a broader audience but is also able to maintain a platform amenable to U.S. initiatives and priorities.

STRATEGIC OBJECTIVE

The CISA international mission depends upon strategic stakeholder engagement to establish a vast, diverse, and robust network of public and private stakeholders and experts in order to promote a collective effort towards protecting critical infrastructure and strengthening the global cyber posture. CISA aims to build and to mature partnerships to create channels of communication that facilitate the exchange of information, best practices, ideas, and lessons-learned as well as to remain timely and relevant on ongoing global efforts to address common issues. Through stakeholder engagement and outreach, CISA is not only able to raise awareness to a broader audience but is also able to maintain a platform amenable to U.S. initiatives and priorities.

DESIRED OUTCOMES

- Greater mutual understanding of the risks, vulnerabilities and other emerging threats to the cyber backbone and critical infrastructure systems and assets between public and private partners.
- Increased understanding and willingness to pursue cooperative activities or bilateral/multilateral arrangements that would foster real-time operational information sharing with priority countries.
- Promotion of CISA's and DHS' best practices and lessons learned that encourages stakeholders to adopt them and thereby increase the security and resilience of critical infrastructure.

Objective 1: Enhance Shared Understanding of Threats and Preparedness for Response

1. Promote U.S. and DHS approaches and resources to managing cybersecurity risk to critical infrastructure, including communications systems, and expand opportunities to discuss the cyber-physical nexus of critical infrastructure security and resilience with international partners.
2. Convene international partners to discuss emerging issues, and actions being taken to mitigate impacts to critical infrastructure while supporting initiatives that are multilateral, enabling CISA to reach a large number of partners through each engagement.
3. Promote U.S. public-private partnership models; processes; and lessons-learned, particularly with countries with overseas assets of interest to the United States.
4. Advance education of the public and pursue international collaboration to promote cybersecurity best practices and maintain an open, interoperable, secure, reliable, and a secure and reliable internet.

STRATEGIC OBJECTIVE

Advance partnerships with industry to further global operational coordination between the public and private sector, when applicable.

DESIRED OUTCOMES

- International approaches to analyzing, assessing, and managing these growing and evolving risks with foreign government and private sector partners will enable us to mature related risk management efforts and identify potential options to harmonize approaches and desired outcomes.
- Build a network of trusted global partners to facilitate exchange of best practices and methodologies, and to discuss emerging priorities to collaborate with like-minded partners, private sector, and civil society on issues of mutual concern.

Objective 2: Advance Global Operational Public-Private Coordination

1. Collaborate with other U.S. government agencies to (1) ensure that various nations' technology-related industrial policies do not have a negative impact on global cybersecurity efforts and (2) pursue efforts to examine such policies, assess the potential impact on global and domestic critical infrastructure, and evaluate our ability to manage the potential impacts from technology related industrial policies.
2. Foster cohesion within the international community on standards and best practices to mitigate against risk as new technology emerges and encourage a level playing field worldwide toward the development of that technology, that imbues certainty and predictability in global markets, while seeking to forestall harmful impacts and increase or sustain innovation.

SHAPING THE POLICY ECOSYSTEM

CISA will ensure that its overall mission and objectives are supported and reflected in a manner consistent with CISA's authorities and U.S. policy goals while shaping the legal environment and effectively driving research and development. By advancing domestic initiatives and promoting national models at the international level, CISA will lead global efforts to support common approaches to shared challenges in securing critical infrastructure and cyberspace. Through cooperation with the Department and the interagency, CISA will guide overall U.S. government efforts to work bilaterally, regionally and multilaterally with foreign counterparts to promote the adoption of standards, regulations and policies that support a homeland and global community that is safe, secure and resilient to threats and hazards.

GOAL 4: SHAPING THE POLICY ECOSYSTEM

Shape a global policy environment that supports U.S. priorities and enables future requirements.

STRATEGIC OBJECTIVE

International engagement must always be considered in the context of larger national security, economic security, and foreign policy goals and objectives. CISA will support and advance U.S. goals and objectives with international partners and through international fora through its unique capabilities, expertise, and authorities. CISA will also collaborate and coordinate with international partners to enhance awareness and ability to systematically address hybrid risks and emerging threats (and their potential impacts) to maintain international stability and develop international standards that guard against risk to ICT and mitigate supply chain risks.

DESIRED OUTCOMES

- International standards that reflect CISA operational priorities and requirements are developed and adopted.
- Relevant multilateral bodies adopt confidence building measures and norms of behavior that advance DHS priorities in cybersecurity and infrastructure security and resilience are adopted by relevant multilateral bodies.
- U.S. policies and regulations are adopted that support CISA priorities and operations and those of its stakeholders.

Objective 1: Advance U.S. Interests in International Fora

1. Promote CISA, DHS, and U.S. Government interests in international venues.
2. Advocate for confidence building measures and norms of behavior that advance global cybersecurity & physical security cooperation, including increasing awareness of – and sensitizing international counterparts to – possible benefits and negative impacts of various policies and procedures on cyber and critical infrastructure while deterring threats from foreign adversaries.
3. Support partner nations' efforts to develop strategies, policies, and programs that both reflect national models and multi-stakeholder models and are in line with CISA's mission and priorities.
4. Promote and contribute to the development and adoption of international standards to strengthen cybersecurity, to fortify critical infrastructure security and resilience, and to improve communications.
5. Partner with the U.S. interagency to influence and to shape international standards that embrace cybersecurity and related norms, enhance resiliency, and mitigate risks.

STRATEGIC OBJECTIVE

Collaborate and coordinate with international partners to enhance awareness and ability to systematically address hybrid risks and emerging threats (and their potential impacts) to maintain international stability.

DESIRED OUTCOMES

- A robust international policy and standards ecosystem that allows the United States to assess and determine an acceptable level of risk to our collective international stability.

Objective 2: Develop Capabilities and Standards that Support U.S. Interests

1. Work through international bodies and partners to enhance the awareness and ability of international partners to systematically address hybrid risks and emerging threats (and their potential impacts) to maintain international stability.
2. Support international efforts to create processes, frameworks, and standards that collectively increase the prevalence and deployment of ICT from trusted vendors in order to reduce the risk of supply chain compromise, whether through next generation technology or adversarial actors.
3. Promote security and resilience by design to ensure that systems, assets, and services are designed with the uninterrupted operating of national critical functions in mind.
4. Decrease the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, which are essential to the conduct of free and fair democratic elections, and the ability of disinformation campaigns to impact elections.

DEFINING PRIORITIES & FORMS OF ENGAGEMENT

EVALUATING ENGAGEMENTS

Evaluating and balancing the application of engagement criteria requires close cooperation across CISA and with interagency partners to ensure relevance to the threat environment. Based on the current needs and leadership's priorities, CISA's Stakeholder Engagement Division's (SED) International Affairs Branch leads CISA's overall international engagement by pursuing bilateral and multilateral international engagement.

Engaging international partners reinforces and amplifies domestic efforts and is vital to executing the Mission to ensure the safety and reliability of U.S. critical infrastructure, including cyber and communications systems. As the CISA mission areas mature, there is both an opportunity and necessity to prioritize engagement with a targeted set of partners in order to achieve a meaningful return on investment. CISA seeks to achieve concrete, measurable outcomes while balancing resource and mission requirements. To this end, the following criteria/rationale are used to guide the prioritization of bilateral partnerships and multilateral venues for cooperation:

Closest Allies: Close allies with a history of deep engagement across all aspects of our government (such as Australia, Canada, New Zealand, and the United Kingdom).

Opportunity to Influence: Countries or organizations with which there is an opportunity to influence and/or shape the trajectory of development of national security capability and for which the U.S. has specific national goals. This includes working with partners who are subject to risks and threats from known adversaries in an effort to mitigate harm.

Peers: Peer countries or organizations with significant technical capability and reciprocal investment in the relationship. This may include robust engagement critical infrastructure protection and partnerships or mitigating cyber incidents, or joint investment in research and development efforts.

Strategic Imperative: Countries or organizations which the United States is pursuing a specific strategic imperative. This may include engagements designed to advance U.S. regional objectives or other national security goals or to understand an adversaries' tactics, techniques, infrastructure security procedures, and cybersecurity policy goals.

In addition, CISA relies on a range of venues to support its international security priorities. Such venues include international, regional, and specialized fora, as well as industry groups with a global membership and outlook. These diverse fora that facilitate cooperation with other government entities and stakeholders from the private sector and civil society are important to building international cooperation and consensus on a range of security issues of mutual interest.

Ultimately, there are multiple factors CISA considers in identifying with whom to collaborate and in what way. This includes:

- **Achieve:** Directly advance a mission and/or programmatic rationale, including the potential for directly increasing the security and resilience of U.S. critical infrastructure including cybersecurity;
- **Build:** Create opportunities for reciprocal benefit for engagement, including learning from – or contributing to – a partner country's technical capability and/or historical relationships;
- **Harmonize:** Promote international policy harmonization or encourage partner countries to join U.S. proposed or supported frameworks; and
- **Influence:** Shape a partner's decision with regard to a technical or policy development, political choice, or similar opportunity, or exchange for other benefit.

SECURING TOMORROW

Global engagement and operations are fundamental to our cybersecurity, infrastructure security, emergency communications, and risk management efforts. These international efforts strengthen our ability to perform our domestic mission, and help advance foreign partner capacity in these areas, thereby strengthening global resiliency.

Given the dynamic threat landscape and significant developments in global cybersecurity and infrastructure security related policies, the U.S. government must remain fully engaged to shape an environment that will preserve our national security interests, economic security interests, and competitiveness into the future. CISA has a key role to play in these efforts and will actively work with international partners to defend today and secure tomorrow.

DEFEND TODAY, SECURE TOMORROW