

U.S. Customs and Border Protection Cybersecurity Strategy

Enabling the Mission Through Secure Technology



U.S. Customs and
Border Protection

Table of Contents

Message from the Commissioner

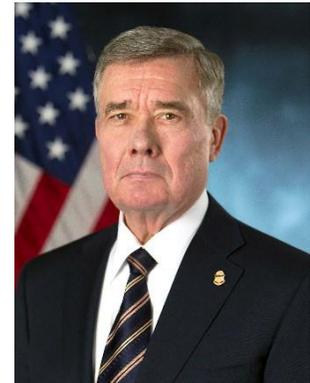
Executive Summary

Introduction	1
Cybersecurity Strategic Goals	3
▪ Protect the CBP Mission and People by Integrating Cybersecurity into the Organization	4
▪ Build a Strong Cybersecurity Foundation and Drive toward Sustainable Mission Integrity	7
▪ Develop and Support a Skilled Workforce	9
Path Forward	11



A Message from the Commissioner

As Federal agencies become increasingly reliant on technology solutions, cyberspace and its underlying infrastructure are essential tools for mission delivery. The government's digital infrastructure, however, is constantly under attacks from malicious actors whose capabilities are growing increasingly sophisticated. Recent breaches of sensitive government systems and the consequences of these breaches have made clear the need for us to reevaluate the Nation's approach to cybersecurity.



In safeguarding America's borders and promoting economic prosperity, U.S. Customs and Border Protection connects its employees to a secure cyberspace network containing sensitive, mission critical information. With CBP's expansion in technology and connectivity over the past 10 years, employees are able to more effectively carry out their duties. This increased connectivity only enhances our organization's effectiveness and the Nation's security if CBP adopts tough cybersecurity measures.

Given the significant potential impacts of a cyber breach, cybersecurity must be a shared responsibility that is a top priority for all CBP employees. Everyone has a part to play in protecting CBP networks, systems, and the traveler and trade data that has been entrusted to us. While we have recently pulled together to achieve great gains in this area, there is still much work to do.

The CBP Cybersecurity Strategy is intended to advance CBP's cybersecurity posture amid continued growth in connectivity by engaging all of CBP in achieving three strategic goals:

- Protect the CBP mission by integrating cybersecurity into the organization;
- Building a strong cybersecurity foundation and drive toward sustainable mission integrity; and
- Develop and support a skilled workforce.

This strategy and its three principal objectives will provide a unified framework to guide coordinated cybersecurity efforts across all CBP offices and help CBP achieve proactive, risk-based cybersecurity posture. Through the implementation of a strong Cybersecurity Strategy, we will better protect this agency and the Nation.

A handwritten signature in black ink that reads "R. Gil Kerlikowske". The signature is written in a cursive, slightly slanted style.

R. Gil Kerlikowske
Commissioner
U.S. Customs and Border Protection



Executive Summary

Technology solutions play a significant role supporting CBP's mission. They ensure the security of our Nation's borders and improve secure travel and trade. While technology and network-enabled capabilities significantly enhance CBP's daily operations, it also increases CBP's vulnerability to external attacks through cyberspace. This creates opportunities for adversaries (e.g., nation states, organized criminals, and terrorists) to use cyber attacks to disrupt CBP's operations and compromise the confidentiality, integrity, and availability of CBP data. For example, an adversary could infiltrate and take command of the CBP's cargo screening systems in a way that would not be apparent to CBP officials, allowing criminals to smuggle contraband into the country undetected. An adversary could also completely shut down CBP's cargo screeners, slowing or even stopping trade through a major shipping port to create a crippling economic effect. A coordinated attack to shut down multiple ports could cause retail store shelves to become bare in less than three days. While these outcomes alone could seriously compromise national security, a cyber and physical attack launched simultaneously could even lead to a loss of life of CBP officers and agents.

CBP's cybersecurity challenge requires the right mix of technology, workforce resources, and procedures to improve its cyber defenses without impacting the operational speed and agility CBP requires to defend the Nation's borders. This strategy provides a framework for CBP to tackle this challenge head on by defining a vision for cybersecurity that provides objectives and initiatives that protects CBP's networks from outside attacks. The strategy also recognizes that each CBP mission area may require unique cybersecurity capabilities, but achieving a strong security baseline requires coordination and recognition that cybersecurity is a shared responsibility of all CBP employees. To that end, CBP has identified three strategic cybersecurity goals:

- i. **Protect the CBP mission and people by integrating cybersecurity into the organization:** CBP has a responsibility to ensure that cybersecurity measures are integrated throughout all of its mission areas through effective governance policies and procedures.
- ii. **Build a strong cybersecurity foundation and work toward sustainable mission integrity:** CBP must achieve a proactive and vigilant cybersecurity posture, ready to quickly respond and recover from a cyber incident so that cyber attacks do not compromise CBP's ability to perform its mission.
- iii. **Develop and support a skilled workforce:** Recruiting, developing, and retaining a cybersecurity workforce that is equipped to work with new technologies and address emerging threats is vital to protect CBP's ability to execute its mission.

CBP will use this strategy to coordinate and guide the cybersecurity activities across each of its offices to create a strong and resilient security posture. Since cybersecurity is a shared responsibility, each office and employee will play a role applying the strategy. As a result of a renewed focus on cybersecurity, CBP's overall security will continue to improve both today and into the future.



Introduction

U.S. Customs and Border Protection (CBP) secures the Nation's borders to ensure the efficient flow of legitimate trade and travel across U.S. borders. More than 60,000 CBP employees maintain over 325 ports of entry and 135 border patrol stations throughout the United States to carry out CBP's mission on the border, at port, in the air, and at sea. CBP's activities significantly influence the U.S. economy, supporting approximately \$2.4 trillion in trade revenue each year. In CBP's critical role assisting the Nation's commerce, any interruption of the flow of goods would harm the country's economy.

From alerting officers to pending threats to screening cargo at ports of entry, CBP relies on a variety of technology solutions to carry out its mission. Systems such as Global Entry, Trusted Trader, and the Automated Commercial Environment connect with passengers, trade partners, and government partners to create efficiencies and improved screening capabilities. Other systems allow border patrol agents to process individuals that cross the border illegally.

CBP's mission, the data that it manages, and its role supporting the U.S. economy make it an attractive target for nation states, drug cartels, organized criminals, and terrorists. As CBP continues to rely on connected, technology-based systems to support its mission, its exposure and vulnerabilities to cyber attacks increases. For example:



- A denial-of-service attack against port screening equipment could make the equipment inaccessible or inoperable, resulting in empty retail store shelves in a matter of days.
- Cyber criminals could take advantage of potential vulnerabilities in scanning equipment to smuggle contraband and illicit materials across the borders.
- Forensic and laboratory data could be stolen or modified without CBP knowledge, compromising ongoing investigations and legal actions, leading to release of criminals and terrorists.

Cybersecurity also plays a critical role protecting the safety of the agency's law enforcement officers and agents. Any technology application that supports CBP officer or agent operations—such as field communications, video surveillance, or GPS—may be susceptible to an attack that could put the integrity of any field operation at risk, and possibly endanger lives. For example, cyber threats could jam radio communications and disrupt data feeds from ground sensors and remote and mobile video surveillance systems, prohibiting CBP agents from communicating.

CBP's strategic cybersecurity goal is closing the gap between increasingly sophisticated and persistent threat actors and CBP's adoption of the right technology, people, and processes. Shifting and competing priorities make it difficult for Federal agencies to maintain state-of-the-art capabilities but, without effective cybersecurity measures, CBP's entire mission is at risk. It is vital that every CBP employee, stakeholder, and partner fully recognize and appreciate the direct connection between sound cybersecurity practices and the national security of the United States.

The CBP Cybersecurity Strategy will help secure CBP's technology assets and protect the mission by implementing proactive, risk-based cybersecurity practices that create a strong and resilient security posture for CBP systems, networks, and data. It also provides an overarching framework for CBP's cybersecurity initiatives and activities. Because each office has diverse operational and technological needs, the activities required to secure each mission area will vary. Despite this, achieving a strong cybersecurity baseline for the entire agency will require coordinating efforts and resources against a single vision, and prioritizing investments based on risk.



Cybersecurity Strategic Goals

A successful cybersecurity program at CBP must balance the need for real-time operational support in a way that safeguards the confidentiality, integrity, and availability of all systems, networks, and personnel. As a result, CBP has established three strategic objectives that support its cybersecurity vision, addressing the people, processes, and tools that are critical to a strong cyber program. Each goal, discussed in the proceeding sections, is supported by a series of objectives and specific initiatives. These are designed to help CBP's executives incorporate elements of the strategy in future planning. Together, these goals, objectives, and initiatives support risk-based cybersecurity management and lay the groundwork for a sound cybersecurity program across the agency, positioning CBP to reduce future threats.



When developing this strategy, CBP referenced existing Federal policy (e.g., National Institute of Standards and Technology guidance and Office of Management and Budget Directives) and the Quadrennial Homeland Security Review, which aims to strengthen the security and resilience of Federal networks and critical infrastructure.¹ CBP's strategic cybersecurity objectives build upon the Department of Homeland Security's (DHS) goals to base cybersecurity actions on risk to achieve a culture of sustainable security. As Federal policy and guidance continues to evolve, CBP will update this strategy.

¹ Department of Homeland Security. 2014 Quadrennial Homeland Security Review. June 2014



I. Protect the CBP Mission and People by Integrating Cybersecurity into the Organization

CBP has a responsibility to ensure that cybersecurity and privacy protections are included throughout all of its mission areas through effective governance, policies, and procedures without hindering the mission.

Objective 1: Support Risk-Based Decision-Making and Prioritize High-Value and Sensitive Assets

CBP systems are under constant attack. Even with unlimited resources and the latest technologies, the pace of technological change and increasing hacker sophistication means that there is always the possibility that a highly-motivated adversary could penetrate some part of the CBP network. To reduce the probability and impact of a mission-critical breach, CBP leaders must use a risk-based approach to cybersecurity planning, ensuring that the most sensitive data and systems are prioritized for protection and hardening.

- **Initiative 1.1: Instill in the organization a clear understanding of the connection between information technology and mission effectiveness**

CBP must understand the systems, resources, hardware, and software that it relies on every day, as well as their configurations. An incomplete understanding of CBP’s assets could lead to misallocation of resources or improper asset deployment, which could leave CBP vulnerable to cyber attacks. To this end, CBP will consolidate its disparate IT asset inventories and standardize configurations to support better cybersecurity planning and actions.

- **Initiative 1.2: Prioritize capabilities and investments to protect CBP’s highest risk assets**

Once an accurate IT asset inventory is established, CBP leaders will determine a risk score for each asset. Based on this scoring exercise, CBP can apply resources to those systems deemed most critical for protection. As CBP acquires new technologies, it will continue to maintain and update the IT asset inventories and monitor risk.

Objective 2: Build Cybersecurity into Future Planning

Cybersecurity must be integrated into future technology planning and considered when evaluating new and emerging technologies. Otherwise, CBP risks acquiring systems that are unsupported (or not well-supported) by CBP’s cybersecurity infrastructure. Deploying technologies without understanding how they affect security, or adopting cyber tools and infrastructure that are not compatible to future technology requirements, increases cybersecurity risks.





- **Initiative 2.1: Institute procurement practices that support supply chain integrity and cybersecurity**

CBP not only relies on vendors to provide general IT solutions and infrastructure, but also specific technologies such as mobility solutions, cargo screening equipment, and biometric readers. When acquiring new technologies, CBP will include cybersecurity requirements in acquisition planning, solicitations, and contract administration, and create appropriate contract oversight and enforcement mechanisms. CBP will prioritize working with vendors that incorporate supply chain risk management practices to maintain the integrity of each component of the supply chain.

- **Initiative 2.2: Incorporate technology refresh cycles and emerging technologies into programmatic plans**

Maintaining technologies that are no longer supported by vendors leads to open and unpatched vulnerabilities that put CBP at risk. Developing plans that include a technology refresh program to replace legacy technology that anticipate new technologies leads to greater security, long-term efficiency, and more accurate budget forecasts.

- **Initiative 2.3: Account for cybersecurity resources when developing budgets**

Using a risk-based approach, CBP’s leaders will build cybersecurity considerations—from procurement to maintenance—into their budget cycles and spending plans. When formulating budget, leaders should consider anticipated staff needs, training resources, costs of updating applications and infrastructure, and acquiring or developing new capabilities.

Objective 3: Develop Appropriate Governance, Oversight, and Compliance Structures

An effective cybersecurity strategy must be supported by appropriate governance structures that promote accountability and compliance with Federal requirements. It is also key that CBP’s governance and management approach be communicated across CBP.

- **Initiative 3.1: Institute clear lines of governance and oversight**

CBP will ensure that its policies, management, and standards related to cybersecurity activities, such as strategy, architecture, and training, are clearly defined and communicated throughout the organization. In order to drive progress, CBP must support its employees responsible for these activities and give them the authority to enforce cybersecurity policies.





- **Initiative 3.2: Achieve compliance with Federal regulations and alignment with best practices**

All Federal agencies must comply with specific security and privacy regulations, including those set by the National Institute for Standards and Technology and the Office of Management and Budget. CBP must also comply with regulations set by DHS. As CBP conducts cybersecurity planning and operations, it will ensure that required security and privacy measures are integrated from initial system development through final decommission.

Objective 4: Broadly Communicate CBP’s Cybersecurity Goals to Federal and Private Sector Partners and Enable Effective Information Sharing

- **Initiative 4.1: Increase all partners’ awareness of the connection between CBP’s mission and cybersecurity**

As part of its mission to support trade and travel, CBP interacts with thousands of stakeholders every day. CBP strives to educate all of its partners on how it is incorporating cybersecurity and privacy protections into existing requirements and programs. This will help protect the integrity and privacy of sensitive data, as well as instill greater public confidence in CBP operations. Similarly, CBP should use existing DHS information sharing programs to collect and share cybersecurity threat information with key stakeholders to raise awareness and reduce threats.

- **Initiative 4.2: Maintain an ongoing dialogue on cybersecurity with government partners**

CBP’s mission requires it to work closely with other Federal agencies, such as U.S. Immigration and Customs Enforcement, to share data and information. CBP must continue to collaborate with other agencies to strengthen its partnerships as well as leverage Federal information sharing programs to share best practices, threat information, and security solutions.





II. Build a Strong Cybersecurity Foundation and Drive toward Sustainable Mission Integrity

Specialized tools and capabilities, such as software and applications, can help CBP achieve a mature and resilient cybersecurity program. When implemented with the right people and processes, proper tools can help CBP anticipate cyber events and be resilient before an attack occurs.

Objective 1: Promote Basic Cyber Hygiene

Cyber hygiene refers to basic practices that users can take to secure their systems, such as regularly updating systems antivirus protections and software. Promoting cyber hygiene principles is an effective and cost efficient way for CBP to keep its networks safe.

- **Initiative 1.1: Patch and update systems regularly**

CBP will follow regular patching cycles for all software and applications, including those installed on network peripheral devices, such as non-intrusive inspection equipment and mobile devices. As part of CBP's risk management process, any system with a granted exception to mandated patching cycles will be regularly reviewed to understand the ongoing vulnerabilities that the exception introduces.

- **Initiative 1.2: Implement rigorous access management**

CBP will ensure that only those with permission to access systems and resources have the ability to do so. This will be accomplished through strong identity management and multi-factor authentication processes—using the DHS personal identity verification (PIV) card and other technologies—to prevent unauthorized network access and maintain a record of user activities. CBP will follow the guidance in the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, which discusses how the government should manage identity, credentialing, and network access.

Objective 2: Proactively Monitor and Protect Networks

CBP must regularly test safeguards and remain vigilant to malicious activity on its networks at all times, as attacks can occur without warning and from unknown attackers.

- **Initiative 2.1: Institute a defense-in-depth posture across CBP's assets**

Defense-in-depth is a comprehensive strategic approach that calls for an organization to separately protect each layer of its information technology infrastructure from the network perimeter to individual data points. This approach helps organizations protect information and technology even if a single security



layer has been compromised. Applying a defense-in-depth strategy with a risk-based approach can better protect CBP's most critical assets from various threats.

- **Initiative 2.2: Maintain continuous insight into network operations**

CBP will continue to implement a continuous diagnostics and mitigation (CDM) solution to not only meet Federal requirements, but also improve CBP's overall cybersecurity by providing real-time insight into network operations. This will help CBP automate alerts, scans, and patches and move toward a future state that proactively and automatically responds to identified threats.

- **Initiative 2.3: Regularly test network security**

To build on CBP's cybersecurity foundation, CBP will increase the use of teams to regularly conduct internal and external vulnerability assessments. As existing vulnerabilities are identified, CBP will continue to rapidly apply the lessons learned to mitigate future vulnerabilities.

Objective 3: Institute Rapid Response and Recovery Procedures

System recovery is critical to continuity of operations. Resilience, the ability to quickly recover from and reduce the impact of cyber incidents, is crucial to CBP's mission effectiveness. CBP must have procedures in place to recover from a cyber attack so that it can avoid having shutting down networks and automated systems for extended periods while the issue is addressed. Shutting down networks would lead to massive inefficiencies and could introduce other security threats (for example, officers working more quickly to move passengers and cargo manually using paper forms, leading to greater risk of human error). Furthermore, significant economic impacts may be felt after mere minutes of an outage.

- **Initiative 3.1: Back up data frequently, with a focus on critical data**

CBP will continue to evaluate and enforce data recovery requirements for all CBP systems, especially for those that would have the greatest effect on CBP operations if they were degraded. CBP will also periodically test back-up systems to confirm they are fully functioning.

- **Initiative 3.2: Exercise disaster recovery plans regularly and ensure lessons learned are incorporated**

Disaster recovery exercises allow CBP to confirm that the right policies, procedures, and lines of communication are in place and will operate as planned when responding to or recovering from a cyber attack. Without regular exercises and a way to incorporate lessons learned, CBP not only jeopardizes its networks and data, but increases the time needed to recover from an attack and resume normal operations.



III. Develop and Support a Skilled Workforce

Each of CBP's 60,000 employees play a critical role in leading, implementing, and maintaining effective cybersecurity, regardless of whether they are in the field or an office. Engaging and educating all employees through role-based training is critical to maintaining a strong cybersecurity posture. Additionally, recruiting, developing, and retaining a cyber workforce that is equipped to work with new technologies and counter emerging threats is vital to protecting CBP's mission.

Objective 1: Engage the CBP Workforce in the Broader Cybersecurity Vision

Cybersecurity is a shared responsibility that must be understood as such by all CBP employees. CBP employees should understand the basic tenets of the CBP Cybersecurity Strategy to help defend against and reduce the impact of a cyber attack. This requires directly engaging the workforce to emphasize the importance of individuals' cybersecurity responsibilities in their jobs.

- **Initiative 1.1: Communicate the cybersecurity vision**

Leadership must effectively communicate the cybersecurity vision to staff and help them understand how cybersecurity is tied directly to the mission. This includes a discussion of various cyber attack scenarios and the potential impacts on mission operations, physical security, and privacy. Personnel should understand how their jobs would be affected under each of these scenarios and the role they would play in either helping to prevent or respond to an attack.

- **Initiative 1.2: Integrate cyber risk management practices into job functions**

Given cybersecurity's role as a key mission enabler across CBP, IT and program managers often find themselves responsible for implementing cybersecurity measures for the first time. All CBP personnel must consider cyber activities essential to their daily roles. Furthermore, individuals who are responsible for key cybersecurity decisions and activities need the authority to enforce cybersecurity requirements across their organizations.

Objective 2: Develop a Workforce to Support Evolving Cybersecurity Needs

A well-prepared cyber workforce serves as the foundation for any agency's cybersecurity program. It provides the agency with the expertise required to carry out cybersecurity plans and is the first line of defense for social engineering cyber attacks (e.g., spear phishing by sending a malicious link through an unsolicited email).





- **Initiative 2.1: Define clear roles and responsibilities for cybersecurity activities**

CBP will assign and communicate clear roles and responsibilities for cybersecurity. CBP will also encourage collaboration across the agency. Specific emphasis should be placed on sharing knowledge and best practices among professionals with similar skills and responsibilities.

- **Initiative 2.2: Employ proactive workforce planning to ensure a skilled cyber workforce**

It is critical that CBP have staff with the right skills to support cybersecurity roles. CBP will approach cybersecurity workforce planning by anticipating future changes in the technical and threat landscape and making sure that it has the right resources for that environment.

- **Initiative 2.3: Provide training and education opportunities**

For cybersecurity personnel, CBP will support training and education that addresses current and evolving threats, as well as how to securely deploy new technologies. Additional educational opportunities will provide cyber personnel exposure to other government, non-profit and academic environments.



Path Forward

CBP will use this strategy to coordinate and guide the cybersecurity activities across its offices. It is a roadmap to achieving a future state in which:

- System vulnerabilities are continuously identified and remediated;
- Technology, workforce, and budget planning are anticipated with cybersecurity in mind;
- Cybersecurity resources are prioritized based on risk; and
- Offices and individuals are accountable for achieving cybersecurity results.

In turn, these activities will help reduce cyber threats to CBP's passenger and cargo screening systems, border operations, and air and marine support, among others.

To achieve these results, the CBP deputy commissioner will leverage a cybersecurity working group with representatives from every mission area to collaborate on cybersecurity planning. Reporting directly to the deputy commissioner's office, this group will help CBP collaborate and bring an agency-level view to cybersecurity resourcing decisions. A successful strategy will protect CBP's data, its operational mission, the U.S. economy, and the safety of the American people.





U.S. Customs and
Border Protection