U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY STRATEGY

INTRODUCTION

We depend upon cyberspace for daily conveniences, critical services, and economic prosperity. At the U.S. Department of Homeland Security, we believe that cyberspace can be made secure and resilient. DHS works with key partners across the Federal government, State and local governments, industry, and the international community to identify and manage national cybersecurity risks. The DHS Cybersecurity Strategy sets out five pillars of a DHS-wide risk management approach and provides a framework for executing our cybersecurity responsibilities and leveraging the full range of the Department's capabilities to improve the security and resilience of cyberspace.

Reducing our national cybersecurity risk requires an innovative approach that fully leverages our collective capabilities across the Department and the entire cybersecurity community. DHS will strive to better understand our national cybersecurity risk posture, and engage with key partners to collectively address cyber vulnerabilities, threats, and consequences. We will build on ongoing efforts to reduce and manage vulnerabilities of federal networks and critical infrastructure to harden them against attackers. We will reduce threats from cyber criminal activity through prioritized law enforcement intervention. We will seek to mitigate the consequences from cybersecurity incidents that do occur. Finally, we will engage with the global cybersecurity community to strengthen the security and resiliency of the overall cyber ecosystems by addressing systemic challenges like increasingly global supply chains; by fostering improvements in international collaboration to deter malicious cyber actors and build capacity; by increasing research and development, and by improving our cyber workforce.

Through these efforts we seek to create a safe and secure cyberspace for the American people and protect the open, interoperable, secure and resilient Internet.

Homeland Security

DHS CYBERSECURITY GOALS

Pillar I
Risk Identification

Goal 1: Assess Evolving Cybersecurity Risks.

We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.

Pillar II
Vulnerability Reduction

Goal 2: Protect Federal Government Information Systems.

We will reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.

Goal 3: Protect Critical Infrastructure.

We will partner with key stakeholders to ensure that national cybersecurity risks are adequately managed.

Pillar III
Threat Reduction

Goal 4: Prevent and Disrupt Criminal Use of Cyberspace.

We will reduce cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.

Pillar IV
Consequence Mitigation

Goal 5: Respond Effectively to Cyber Incidents.

We will minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.

Pillar V
Enable Cybersecurity Outcomes

Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem.

We will support policies and activities that enable improved global cybersecurity risk management.

Goal 7: Improve Management of DHS Cybersecurity Activities.

We will execute our departmental cybersecurity efforts in an integrated and prioritized way.

Homeland Security

OUR CYBERSECURITY STRATEGY IN ACTION

- In October 2017, DHS issued Binding Operational Directive 18-01, mandating that Federal agencies take specific steps to enhance email and web security, including the deployment of DMARC (Domain-based Message Authentication, Reporting and Conformance).
- During the 2017 WannaCry worldwide malware attack, the National Protection and Programs Directorate (NPPD) partnered with other agencies and industry to assist U.S. hospitals to ensure their systems were not vulnerable, and issued a public technical alert to assist defenders with defeating this malware.
- In January 2018, the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and the Department of Justice in Las Vegas indicted 36 individuals for their roles in the Infraud Organization, an internet-based criminal enterprise engaged in the large scale acquisition and sale of stolen credit card data and identity documents. This organization was responsible for the loss in excess of $530 million. The HSI investigation has led to the recovery of over 4.3 million compromised credit card account numbers.
- In July 2017, the United States Secret Service, through a synchronized international law enforcement operation, affected the arrest of a Russian national alleged to have operated BTC-e. From 2011 to 2017, BTC-e is alleged with facilitating over $4 billion worth of bitcoin transactions worldwide for cyber criminals engaging in computer hacking, identity theft, ransomware, public corruption, and narcotics distribution. Researchers estimate approximately 95% of ransomware payments were laundered through BTC-e.
- In October 2017, the U.S. Coast Guard (USCG) stood up the Office of Cyberspace Forces, to organize, man, train, and equip the USCG cyberspace operational workforce and develop cyberspace operational policy to operate, maintain, defend, and secure USCG systems and networks, enable USCG operations through cyberspace capabilities, and protect the Maritime Transportation System from cyber threats.