Fact Sheet: Cybersecurity Legislative Proposal

We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control… But just as we failed in the past to invest in our physical infrastructure – our roads, our bridges and rails – we've failed to invest in the security of our digital infrastructure… This status quo is no longer acceptable – not when there's so much at stake. We can and we must do better. – President Obama, May 29, 2009

Our critical infrastructure – such as the electricity grid, financial sector, and transportation networks that sustain our way of life – have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade. The President has thus made cybersecurity an Administration priority. When the President released his Cyberspace Policy Review almost two years ago, he declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." The Administration has since taken significant steps to better protect America against cyber threats. As part of that work, it has become clear that our Nation cannot fully defend against these threats unless certain parts of cybersecurity law are updated.

Members of both parties in Congress have also recognized this need and introduced approximately 50 cyber-related bills in the last session of Congress. Senate Majority Leader Reid and six Senate committee chairs thus wrote to the President and asked for his input on cybersecurity legislation. The Administration welcomed the opportunity to assist these congressional efforts, and we have developed a pragmatic and focused cybersecurity legislative proposal for Congress to consider. This legislative proposal is the latest achievement in the steady stream of progress we are making in securing cyberspace and completes another near-term action item identified in the Cyberspace Policy Review.

The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

Protecting the American People

1) National Data Breach Reporting. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements.

2) Penalties for Computer Criminals. The laws regarding penalties for computer crime are not fully synchronized with those for other types of crime. For example, a key tool for fighting organized crime is the Racketeering Influenced and Corrupt Organizations Act (RICO). Yet RICO does not apply to cyber crimes, despite the fact that cyber crime has become a big business for organized crime. The Administration proposal thus clarifies the penalties for computer crimes, synchronizes them with other crimes, and sets mandatory minimums for cyber intrusions into critical infrastructure.

Protecting our Nation's Critical Infrastructure

Our safety and way of life depend upon our critical infrastructure as well as the strength of our economy. The Administration is already working to protect critical infrastructure from cyber threats, but we believe that the following legislative changes are necessary to fully protect this infrastructure:

1) Voluntary Government Assistance to Industry, States, and Local Government. Organizations that suffer a cyber intrusion often ask the Federal Government for assistance with fixing the damage and for advice on building better defenses. For example, organizations sometimes ask DHS to help review their computer logs to see when a hacker broke in. However the lack of a clear statutory framework describing DHS's authorities has sometimes slowed the ability of DHS to help the requesting organization. The Administration proposal will enable DHS to quickly help a private-sector company, state, or local government when that organization asks for its help. It also clarifies the type of assistance that DHS can provide to the requesting organization.

2) Voluntary Information Sharing with Industry, States, and Local Government. Businesses, states, and local governments sometimes identify new types of computer viruses or other cyber threats or incidents, but they are uncertain about whether they can share this information with the Federal Government. The Administration proposal makes clear that these entities can share information about cyber threats or incidents with DHS. To fully address these entities' concerns, it provides them with immunity when sharing cybersecurity information with DHS. At the same time, the proposal mandates robust privacy oversight to ensure that the voluntarily shared information does not impinge on individual privacy and civil liberties.

3) Critical Infrastructure Cybersecurity Plans. The Nation's critical infrastructure, such as the electricity grid and financial sector, is vital to supporting the basics of life in America. Market forces are pushing infrastructure operators to put their infrastructure online, which enables them to remotely manage the infrastructure and increases their efficiency. However, when our infrastructure is online, it is also vulnerable to cyber attacks that could cripple essential services. Our proposal

emphasizes transparency to help market forces ensure that critical-infrastructure operators are accountable for their cybersecurity.

The Administration proposal requires DHS to work with industry to identify the core critical-infrastructure operators and to prioritize the most important cyber threats and vulnerabilities for those operators. Critical infrastructure operators would develop their own frameworks for addressing cyber threats. Then, each critical-infrastructure operator would have a third-party, commercial auditor assess its cybersecurity risk mitigation plans. Operators who are already required to report to the Security and Exchange Commission would also have to certify that their plans are sufficient. A summary of the plan would be accessible, in order to facilitate transparency and to ensure that the plan is adequate. In the event that the process fails to produce strong frameworks, DHS, working with the National Institute of Standards and Technology, could modify a framework. DHS can also work with firms to help them shore up plans that are deemed insufficient by commercial auditors.

Protecting Federal Government Computers and Networks

Over the past five years, the Federal Government has greatly increased the effort and resources we devote to securing our computer systems. While we have made major improvements,[1] updated legislation is necessary to reach the Administration goals for Federal cybersecurity, so the Administration's legislative proposal includes:

1) Management. The Administration proposal would update the Federal Information Security Management Act (FISMA) and formalize DHS' current role in managing cybersecurity for the Federal Government's civilian computers and networks, in order to provide departments and agencies with a shared source of expertise.

2) Personnel. The recruitment and retention of highly-qualified cybersecurity professionals is extremely competitive, so we need to be sure that the government can recruit and retain these talented individuals. Our legislative proposal will give DHS more flexibility in hiring these individuals. It will also permit the government and private industry to temporarily exchange experts, so that both can learn from each others' expertise.

3) Intrusion Prevention Systems. Intrusion *detection* systems are automated sensors that identify cyber intrusions and attacks. Intrusion *prevention* systems can actually block cyber intrusions and attacks. DHS' EINSTEIN system is one example of an intrusion prevention system, and the proposal makes permanent DHS's authority to oversee

[1] *See* GAO, .*Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, March 5 2010.

intrusion prevention systems for all Federal Executive Branch civilian computers. Internet Service Providers (ISPs) implement these systems on behalf of DHS, blocking attacks against government computers. The Attorney General currently reviews and provides immunity for those ISPs, as necessary, to provide that service, and the proposal streamlines that process. This only applies to intrusion prevention systems that protect government computers, and the proposal also codifies or adds: strong privacy and civil liberties protections, congressional reporting requirements, and an annual certification process.

4) Data Centers. The Federal Government has embraced cloud computing, where computer services and applications are run remotely over the Internet. Cloud computing can reduce costs, increase security, and help the government take advantage of the latest private-sector innovations. This new industry should not be crippled by protectionist measures, so the proposal prevents states from requiring companies to build their data centers in that state, except where expressly authorized by federal law.

New Framework to Protect Individuals' Privacy and Civil Liberties

The Administration's proposal ensures the protection of individuals' privacy and civil liberties through a framework designed expressly to address the challenges of cybersecurity.

- It requires DHS to implement its cybersecurity program in accordance with privacy and civil liberties procedures. These must be developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All federal agencies who would obtain information under this proposal will follow privacy and civil liberties procedures, again developed in consultation with privacy and civil liberties experts and with the approval of the Attorney General.
- All monitoring, collection, use, retention, and sharing of information are limited to protecting against cybersecurity threats. Information may be used or disclosed for criminal law enforcement, but the Attorney General must first review and approve each such usage.
- When a private-sector business, state, or local government wants to share information with DHS, it must first make reasonable efforts to remove identifying information unrelated to cybersecurity threats.
- The proposal also mandates the development of layered oversight programs and congressional reporting.
- Immunity for the private-sector business, state, or local government is conditioned on its compliance with the requirements of the proposal.

Taken together, these requirements create a new framework of privacy and civil liberties protection designed expressly to address the challenges of cybersecurity.

Conclusion

Our Nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. The Administration has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and we look forward to engaging with Congress as they move forward on this issue.