H.R. 6423, the "Homeland Security Cyber and Physical Infrastructure Protection Act of 2010," as introduced by Reps. Thompson (D-MS), Clarke (D-NY) and, Harman (D-CA)

ONE PAGE SUMMARY

10-17-10

Illegal penetrations or "hacks" of computer networks have become an increasingly serious homeland security issue. Not only do they threaten the personal fortunes and identities of our citizens but also the effective functioning of our government and our infrastructure. Since 2003, when the Department of Homeland Security (DHS) was designated by then-President George W. Bush as the "focal point for the security of cyberspace," (HSPD-7), DHS has not had adequate authority to fulfill its responsibility to protect networks operated by Federal civilian agencies and critical infrastructure. The "Homeland Security Cyber and Physical Infrastructure Protection Act of 2010," seeks to enhance DHS' cybersecurity capacity by authorizing the DHS Office of Cybersecurity and Communications and creating a new Cybersecurity Compliance Division to oversee the establishment of performance-based standards responsive to the particular risks to the (1) .gov domain and (2) critical infrastructure networks, respectively. This bill is designed to require DHS to work with network operators to develop tailored security plans that meet risk-based, performance-based standards, as is being done in DHS' Chemical Facility Anti-terrorism program.

FEDERAL NETWORK SECURITY:

- Authorizes DHS to establish and enforce risk-based, performance-based standards (with corresponding remedies for non-compliance) that were adopted by a newly-created Federal agency working group, comprised of Federal civilian agencies and chaired by the DHS.

- Requires DHS to ensure compliance, and in the case of non-compliance, requires DHS to alert the agency and the Office of Management and Budget, who is then required to administer the remedy.

CRITICAL INFRASTRUCTURE SECURITY (PRIVATE SECTOR):

- Requires DHS to determine which assets should be designated "covered critical infrastructure" and the establishment of a reconsideration process for a firm to challenge such a designation.

- Requires DHS to develop risk-based, performance-based standards, in consultation with key stakeholders, and promulgate those standards through notice and comment.

- Authorizes DHS, acting through HSPD-7-defined "Sector Specific Agencies" or "First Party Regulatory Agencies"[1] as appropriate, to enforce such standards with respect to private sector networks determined to be critical infrastructure.

- Authorizes DHS to recommend (Safety Act) liability protection for firms that comply with the standards and to issue civil penalties of up to $100, 000 per instance of non-compliance.

OTHER PROVISIONS:

- Requires DHS to share, to the greatest extent practical, any relevant threat information with other Federal Agencies and covered companies, (Sec. 3) and requires DHS to ensure that information provided by companies is protected. (Sec. 4).

- Requires DHS to undertake cybersecurity research and development. (Sec. 5).

- Requires DHS to develop a strategic cybersecurity workforce plan, grants limited direct-hire authority to hire an additional 500 cybersecurity professionals, and authorizes retention bonuses for cyber professionals that otherwise would leave DHS. (Sec. 6).

[1] "First Party Regulatory Agency" is defined as a Federal agency that is not a sector specific agency under HSPD 7 but that has primary regulatory authority for a specific critical infrastructure sector or sub-sector.