Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

Eric A. Fischer
Senior Specialist in Science and Technology

December 7, 2011
Summary

For more than a decade, various experts have expressed increasing concerns about cybersecurity, in light of the growing frequency, impact, and sophistication of attacks on information systems in the United States and abroad. Consensus has also been building that the current legislative framework for cybersecurity might need to be revised.

The complex federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure.

More than 50 statutes address various aspects of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place. While revisions to most of those laws have been proposed over the past few years, no major cybersecurity legislation has been enacted since 2002.

Recent legislative proposals, including many bills introduced in the 111th and 112th Congresses, have focused largely on issues in ten broad areas: national strategy and the role of government, reform of the Federal Information Security Management Act (FISMA), protection of critical infrastructure (especially the electricity grid and the chemical industry), cross-sector coordination and information sharing, breaches resulting in theft or exposure of personal data such as financial information, cybercrime, privacy in the context of electronic commerce, international efforts, research and development, and the cybersecurity workforce. For most of those topics, at least some of the bills addressing them proposed changes to current laws. Several of the bills have received committee or floor action, but none have become law.

Three comprehensive legislative proposals on cybersecurity have been presented to the 112th Congress: S. 413, recommendations from a House Republican task force, and a proposal by the Obama Administration. They differ in approach, with S. 413 proposing the most extensive regulatory framework of the three, and the task force recommendations focusing more on incentives for improving private-sector cybersecurity.

All three proposals would revise the Homeland Security Act and increase the statutory responsibilities of the Department of Homeland Security (DHS) for the cybersecurity of federal information systems. They would address vulnerabilities in the information-technology supply chain, enhance public awareness efforts, and address personnel needs to improve the cybersecurity workforce, including providing DHS with broadened personnel authorities. All three would amplify federal efforts in cybersecurity research and development and improve international cooperation in cybersecurity. All would revise FISMA, giving DHS increased authority, stressing the importance of continuous monitoring of systems, and enhancing the compliance-enforcement authorities of agency officials responsible for information systems.
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

Contents

Introduction...................................................................................................................................... 1
Current Legislative Framework.................................................................................................. 1
Executive Branch Actions ......................................................................................................... 3
Legislative Proposals................................................................................................................. 4
Discussion of Proposed Revisions of Current Statutes............................................................ 8
  Posse Comitatus Act of 1879................................................................................................... 10
  Antitrust Laws and Section 5 of the Federal Trade Commission Act.................................. 11
  National Institute of Standards and Technology Act .......................................................... 13
  Federal Power Act ................................................................................................................... 13
  Communications Act of 1934 .................................................................................................. 14
  National Security Act of 1947 ................................................................................................. 15
  U.S. Information and Educational Exchange Act of 1948 (Smith-Mundt Act)................. 16
  State Department Basic Authorities Act of 1956 ............................................................... 17
  Freedom of Information Act (FOIA) ..................................................................................... 17
  Omnibus Crime Control and Safe Streets Act of 1968......................................................... 19
  Racketeer Influenced and Corrupt Organizations Act (RICO) ........................................ 19
  Federal Advisory Committee Act (FACA) .............................................................................. 20
  Privacy Act of 1974................................................................................................................. 20
  Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ......................... 21
  Electronic Communications Privacy Act of 1986 (ECPA) .................................................. 22
  Department of Defense Appropriations Act, 1987 .............................................................. 24
  High Performance Computing Act of 1991 ......................................................................... 25
  Communications Assistance for Law Enforcement Act of 1994 (CALEA) ...................... 26
  Communications Decency Act of 1996 ............................................................................... 27
  Clinger-Cohen Act (Information Technology Management Reform Act) of 1996 ........... 28
  Identity Theft and Assumption Deterrence Act of 1998 .................................................... 29
  Homeland Security Act of 2002 (HSA) .............................................................................. 30
  Federal Information Security Management Act of 2002 (FISMA) ....................................... 32
  Terrorism Risk Insurance Act of 2002 .................................................................................. 34
  Cyber Security Research and Development Act, 2002 ..................................................... 35
  E-Government Act of 2002 .................................................................................................. 36
  Identity Theft Penalty Enhancement Act .............................................................................. 37
  Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA)................................. 38

Tables

Table 1. Topics Addressed by Three Comprehensive Legislative Proposals on Cybersecurity in the 112th Congress .......................................................................................................................... 6
Table 2. Laws Identified as Having Relevant Cybersecurity Provisions .................................. 40

Contacts

Author Contact Information...................................................................................................... 49
Acknowledgments ..................................................................................................................... 49
Introduction

For more than a decade, various experts have expressed concerns about information-system security—often referred to as cybersecurity—in the United States and abroad. The frequency, impact, and sophistication of attacks on those systems has added urgency to the concerns. Consensus has also been growing that the current legislative framework for cybersecurity might need to be revised to address needs for improved cybersecurity, especially given the continuing evolution of the technology and threat environments. This report, with contributions from several CRS staff (see Acknowledgments), discusses that framework and proposals to amend more than 30 acts of Congress that are part of or relevant to it.

Current Legislative Framework

The federal role in addressing cybersecurity is complex. It involves both securing federal systems and fulfilling the appropriate federal role in protecting nonfederal systems. There is as yet no overarching framework legislation in place, but many enacted statutes address various aspects of cybersecurity. Some notable provisions are in the following acts:

---

1 The term information systems is defined in 44 U.S.C. §3502 as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information,” where information resources is “information and related resources, such as personnel, equipment, funds, and information technology.” Thus cybersecurity, a broad and arguably somewhat fuzzy concept for which there is no consensus definition, might best be described as measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from various forms of attack. The concept has, however, been characterized in various ways. For example, the interagency Committee on National Security Systems has defined it as “the ability to protect or defend the use of cyberspace from cyber attacks,” where cyberspace is defined as “a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Committee on National Security Systems, National Information Assurance (IA) Glossary, April 2010, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf). In contrast, cybersecurity has also been defined as synonymous with information security (see, for example, S. 773, the Cybersecurity Act of 2010, in the 111th Congress), which is defined in current law (44 U.S.C. §3532(b)(1)) as

   protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

   (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
   (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
   (C) availability, which means ensuring timely and reliable access to and use of information; and
   (D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access.

Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

- **The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984** prohibits various attacks on federal computer systems and on those used by banks and in interstate and foreign commerce.

- **The Electronic Communications Privacy Act of 1986 (ECPA)** prohibits unauthorized electronic eavesdropping.

- **The Computer Security Act of 1987** gave the National Institute of Standards and Technology (NIST) responsibility for developing security standards for federal computer systems, except the national security systems that are used for defense and intelligence missions, and gave responsibility to the Secretary of Commerce for promulgating security standards.

- **The Paperwork Reduction Act of 1995** gave the Office of Management and Budget (OMB) responsibility for developing cybersecurity policies.

- **The Clinger-Cohen Act of 1996** made agency heads responsible for ensuring the adequacy of agency information-security policies and procedures, established the chief information officer (CIO) position in agencies, and gave the Secretary of Commerce authority to make promulgated security standards mandatory.

- **The Homeland Security Act of 2002 (HSA)** gave the Department of Homeland Security (DHS) some cybersecurity responsibilities in addition to those implied by its general responsibilities for homeland security and critical infrastructure.

- **The Cyber Security Research and Development Act**, also enacted in 2002, established research responsibilities in cybersecurity for the National Science Foundation (NSF) and NIST.

- **The E-Government Act of 2002** serves as the primary legislative vehicle to guide federal IT management and initiatives to make information and services available online, and includes various cybersecurity requirements.

- **The Federal Information Security Management Act of 2002 (FISMA)** clarified and strengthened NIST and agency cybersecurity responsibilities, established a central federal incident center, and made OMB, rather than the Secretary of Commerce, responsible for promulgating federal cybersecurity standards.

More than 40 other laws identified by CRS also have provisions relating to cybersecurity (see Table 2). Revisions to many of those laws have been proposed. More than 40 bills and resolutions with provisions related to cybersecurity have been introduced in the first session of the 112th Congress, including several proposing revisions to current laws. In the 111th Congress, the total was more than 60. Several of those bills received committee or floor action, but none

---

3 This term is defined in 44 U.S.C. §3542(b)(2).

4 Those bills were identified through a two-step process—candidates were found through searches of the Legislative Information System (LIS, http://www.congress.gov) using “cybersecurity,” “information systems,” and other relevant terms in the text of the bills, followed by examination of that text in the candidates to determine relevance for cybersecurity. Use of other criteria may lead to somewhat different results. For example, using the LIS “cybersecurity” topic search yields about 30 bills in the 112th Congress and 40 in the 111th, with about a 50% overlap in the bills included. While that difference is higher than might be expected, none of the bills identified uniquely by the LIS topic search are relevant to the discussion in this report.
have become law. In fact, no comprehensive cybersecurity legislation has been enacted since 2002.5

**Executive Branch Actions**

Some significant executive actions have been taken, however. The George W. Bush Administration established the Comprehensive National Cybersecurity Initiative (CNCI) in 2008 through National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Those documents are classified, but the Obama Administration released a description of them in March 2010.6 Goals of the 12 subinitiatives in that description include consolidating external access points to federal systems; deploying intrusion detection and prevention systems across those systems; improving research coordination and prioritization and developing “next-generation” technology, information sharing, and cybersecurity education and awareness; mitigating risks from the global supply chain for information technology; and clarifying the federal role in protecting critical infrastructure.

In December 2009, the Obama Administration appointed Howard Schmidt to the position of White House Cybersecurity Coordinator.7 He is a member of the White House national security staff and is responsible for government-wide coordination of cybersecurity, including the CNCI. One of the most visible initiatives in which he has been involved is the implementation of automated, continuous monitoring of federal information systems.8 Other stated priorities include developing a unified strategy for network security and incident response, and strengthening partnerships with the private sector and other countries. He works with both the National Security and Economic Councils in the White House. However, the position has no direct control over agency budgets, and some observers argue that operational entities such as the National Security Agency (NSA) have far greater influence and authority.9 The Obama Administration has also launched several initiatives.10

---

5 Among the broader proposals in the 111th Congress, S. 773 (S.Rept. 111-384) and S. 3480 (S.Rept. 111-368) were reported by the originating committees. H.R. 4061 (H.Rept. 111-405) and H.R. 5136 (Title XVII, mostly similar to H.R. 4900) both passed the House. A bill combining provisions of the two Senate bills was drafted (Tony Romm, “Lack of Direction Slows Cybersecurity,” Politico, November 4, 2010, http://www.politico.com/news/stories/1110/44662.html). In the 112th Congress, S. 413 is similar to S. 3480 in the previous Congress, H.R. 2096 (H.Rept. 112-264) is similar to H.R. 4061, and the Senate combined draft is reportedly still being developed (Gautham Nagesh, “Reid Says Senate Will Take Up Cybersecurity Bill Next Year,” Hillicon Valley, November 17, 2011, http://thehill.com/blogs/hillicon-valley/technology/194245-senate-will-take-up-cybersecurity-bill-next-year).


7 The position has been popularly called the “cyber czar.”


Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector. Cross-agency responsibilities are complex, and any brief description is necessarily oversimplified. In general, in addition to the roles of White House entities, DHS is the primary civil-sector cybersecurity agency. NIST, in the Department of Commerce, develops cybersecurity standards and guidelines that are promulgated by OMB, and the Department of Justice is largely responsible for the enforcement of laws relating to cybersecurity.\(^{11}\) The National Science Foundation (NSF), NIST, and DHS all perform research and development (R&D) related to cybersecurity. The National Security Agency (NSA) is the primary cybersecurity agency in the national security sector, although other agencies also play significant roles. The recently established U.S. Cyber Command, part of the U.S. Strategic Command in the Department of Defense (DOD), has primary responsibility for military cyberspace operations.

**Legislative Proposals**

In general, legislative proposals on cybersecurity in the 111\(^{\text{th}}\) and 112\(^{\text{th}}\) Congresses have focused largely on issues in ten broad areas:

- national strategy and the role of government,
- reform of FISMA,
- protection of critical infrastructure (especially the electricity grid and the chemical industry),
- cross-sector coordination and information sharing,
- breaches resulting in theft or exposure of personal data such as financial information,
- cybercrime offenses and penalties,
- privacy in the context of electronic commerce,
- international efforts,
- research and development, and
- the cybersecurity workforce.

For most of those topics, at least some of the bills addressing them proposed changes to current laws.

There appears to be considerable support in principle for significant legislation to address most of those issues. The House, Senate, and White House have taken somewhat different approaches to

(...continued)

\(^{11}\) This responsibility is shared to some extent with other agencies such as the U.S. Secret Service.
such legislation. The Senate has been working since last year on developing a comprehensive bill synthesizing approaches proposed by the Homeland Security and Governmental Affairs Committee, the Commerce, Science, and Transportation Committee, and others, but that proposal is not publically available.

Three comprehensive legislative proposals have been presented to the 112th Congress. As outlined in Table 1, all address most of the issues listed above, although in different ways. S. 413, the Cybersecurity and Internet Freedom Act of 2011 (known also as the Lieberman/Collins bill), introduced in February 2011, is similar to S. 3480 from the 111th Congress. In April 2011, the White House sent a comprehensive, seven-part legislative proposal (White House Proposal) to Congress. In October, the 12-Member House Republican Cybersecurity Task Force, which had been formed by Speaker Boehner in June, released a series of recommendations (Task Force Report) to be used by House committees in developing cybersecurity legislation. Unlike the other two proposals, it was not presented in the form of a bill or bills.

All three proposals would revise the HSA. They would address vulnerabilities in the information-technology supply chain, enhance public awareness efforts, and address personnel needs to improve the cybersecurity workforce, including providing DHS with enhanced personnel authorities. All three would enhance federal efforts in cybersecurity R&D and increase the statutory responsibilities of DHS for the cybersecurity of federal information systems.

S. 413 and the White House Proposal would establish a capability within DHS that would have incident-reporting and other duties. All three also propose improved international cooperation in cybersecurity, but the Task Force Report goes further, calling for U.S. leadership in developing international instruments, similar to those used for terrorism and narcotics trafficking, to prevent and punish malicious cyber-activities.

All would revise FISMA, giving DHS increased authority, stressing the importance of continuous monitoring of systems, and enhancing the compliance-enforcement authorities of agency officials responsible for information systems. S. 413 and the White House Proposal would transfer authorities and functions for information security policy from OMB to DHS. Both provide authority to DHS to ensure compliance with requirements, and stress security testing and mitigation of vulnerabilities. Both eliminate the current FISMA provision giving OMB responsibility for ensuring operation of a federal incident center. Both also transfer the

---

12 See footnote 5.
15 S. 413 and the White House Proposal focus on DHS R&D, while the Task Force Report recommendations also involve several other agencies.
17 It does not, however, call specifically for legislation relating to this recommendation.
responsibility for promulgating information-security standards for federal systems from OMB to the Department of Commerce.\(^\text{18}\)

**Table 1. Topics Addressed by Three Comprehensive Legislative Proposals on Cybersecurity in the 112th Congress**

<table>
<thead>
<tr>
<th>Topic</th>
<th>S. 413</th>
<th>White House Proposal</th>
<th>Task Force Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expansion of DHS authorities for federal systems</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>New office/center</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>US-CERT or related capabilities</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Personnel authorities for cybersecurity</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Supply-chain vulnerabilities</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>FISMA reform</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Protection of privately held critical infrastructure (CI)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Government/private-sector collaboration on CI protection</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>New public/private entity</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Additional regulation of privately held critical infrastructure</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FOIA exemption for cybersecurity information</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Cybersecurity R&amp;D</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Public awareness</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cybercrime law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data breach notification</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Internet security provider code of conduct</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White House cybersecurity office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency measures</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>National Security/Defense and Civil Sector Coordination</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: CRS.

\(^{18}\) This authority had been granted to the Secretary of Commerce under the Clinger-Cohen Act of 1996 (P.L. 104-106) but was transferred to the Director of OMB by the FISMA title in the HSA in 2002 (P.L. 107-296, Sec. 1002, 40 U.S.C. §11331). Note that the version of the Chapter 35 provisions that is currently in effect (Subchapter III) was enacted by the FISMA title in the E-Government Act of 2002 (P.L. 107-347, Title III), but that is not the case for 40 U.S.C. §11331, for which the version in the E-Government Act would have retained the authority of the Secretary of Commerce to promulgate those standards, even though it was enacted after the HSA. The reason for this potentially confusing difference appears to be that (1) the effective date of HSA was later than that of the E-Government Act, and (2) HSA changed 44 U.S.C. Chapter 35 by amending the existing subchapter II, which the E-Government Act explicitly suspended.
Both S. 413 and the *White House Proposal* would also require DHS to issue and enforce regulations for meeting of cybersecurity requirements by private-sector critical infrastructure entities. The *Task Force Report* recommends that Congress consider targeted and limited additional regulation of highly regulated industries where required to improve cybersecurity. S. 413 provides for civil penalties for noncompliance, but the *White House Proposal* prohibits the imposition of monetary liabilities. Both that proposal and the *Task Force Report* establish a FOIA exemption for cybersecurity information, but S. 413 does not. For most of critical infrastructure, however, the *Task Force Report* recommends that Congress adopt a menu of voluntary incentives and facilitate the establishment of a nongovernmental clearinghouse for sharing cybersecurity information between the private sector and the federal government. A draft bill being considered by the House Committee on Homeland Security would create such an organization.

The *White House Proposal* and the *Task Force Report* would each revise current criminal statutes relating to cybersecurity, including criminalizing the damaging of computers associated with critical infrastructure (CI). They would also both set federal requirements for data breach notification—public notification in cases where a security breach poses significant risks of exposure of sensitive personal information.

One of the major provisions of S. 413 is unique among the three proposals. Like some other bills, it would establish a White House cybersecurity office responsible for national cybersecurity strategy and oversight of federal activities, with appointment of the director requiring Senate confirmation. S. 413 would also permit the President to declare a national cybersecurity emergency in response to an imminent threat to covered CI and to take actions consistent with response plans, but it bars the President or other representatives of the federal government from shutting down the Internet. The *White House Proposal* has a related but more restricted provision that focuses on federal systems and does not appear to permit direct actions relating to privately held CI. It permits the Secretary of Homeland Security to respond to threats or incidents by requiring agency actions aimed at protecting federal systems, and to respond to an imminent threat by taking lawful actions relating to transmission of federal information.

The *Task Force Report* also addresses some matters not covered by the other two documents. It proposes that Congress clarify the authority and responsibility of the federal government to protect private information systems and the roles of the military and intelligence communities in cyberspace, including Defense Support of Civil Authorities, but it does not make any specific

---

19 Among the possibilities discussed are tying adoption of standards to incentives such as grants and streamlined regulation, using tax credits, and facilitating the development of a cybersecurity insurance market.


22 For example, H.R. 1136 would establish a White House cybersecurity office as part of an extensive revision of FISMA. S. 778 in the 111th Congress would also have established such an office, although not as part of an explicit revision to current law.

23 Section 2 did not appear in S. 3480, the version of this bill in the 111th Congress. It was added in response to a controversy about whether the emergency powers granted to the President by the bill, or powers granted by the Communications Act of 1934 (47 U.S.C. §606), included the authority to shut down privately run Internet operations.

recommendations on those topics, except to propose that DOD leverage technology transfer and training to increase support to other agencies.\(^{25}\) It also proposes that Internet service providers (ISPs) develop and adopt industry-wide codes of conduct for enhancing cybersecurity protections for their customers.\(^{26}\)

**Discussion of Proposed Revisions of Current Statutes**

To identify laws that might be considered candidates for revision, CRS conducted a broad search, consulting with various experts and examining various sources, including legislative proposals in the 111th and 112th Congresses. That search yielded more than 50 potentially relevant statutes (see Table 2), of which proposed revisions were identified for 31.\(^{27}\) For each of the latter group, the report contains an entry that includes

- the popular name of the statute;\(^{28}\)
- the public law number, along with Statutes-at-Large and relevant U.S. Code citations;\(^{29}\)
- a brief description of the relevance of the statute for cybersecurity;\(^{30}\) and
- discussion of potential revisions or updates that have been suggested.\(^{31}\)

\(^{25}\) DOD and DHS have initiated an interdepartmental collaborative and support agreement on cybersecurity under existing authorities, but the agreement does not involve other agencies (Department of Homeland Security and Department of Defense, “Regarding Cybersecurity,” Memorandum of Agreement, October 13, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf).


\(^{27}\) There are 27 entries, but the one on antitrust laws consists of four different statutes. Neither of the two lists is intended to be definitive or exhaustive. For example, some analysts may argue that more agency authorization statutes should be included, or, alternatively, that some of the statutes that are included are not of significant relevance.

\(^{28}\) This is the name by which the statute is commonly known.

\(^{29}\) The public law (P.L.) and *United States Statutes at Large* (Stat.) citations refer to the original law to which the popular name currently applies. Laws enacted before 1957 generally do not have public law numbers but chapter numbers (Ch.) instead. U.S. Code (U.S.C.) citations refer to the codified law, including any amendments, of those provisions deemed most relevant for cybersecurity as discussed in the text under that law (see also footnote 30). For more information about citation forms, see Law Library of Congress, “Federal Statutes,” April 4, 2011, http://www.loc.gov/law/help/statutes.php. More complete cross-references of public laws to corresponding provisions of U.S. Code can be found in classification tables (see, for example, U.S. House of Representatives, Office of the Law Revision Counsel, “U.S. Code Classification Tables,” 2011, http://uscode.house.gov/classification/tables.shtml).

\(^{30}\) In some cases, such as the Cybersecurity Research And Development Act, P.L. 107-305, the entire statute is relevant to cybersecurity. In others, such as the Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, the statute has a broader focus and only the provisions relevant to the text are cited and described. However, given that cybersecurity is not a precise concept, there may in some cases be legitimate disagreements among experts about which provisions are relevant. Therefore, the descriptions and U.S. Code citations cannot be considered definitive.

\(^{31}\) The discussion is provided for purposes of information only. CRS does not propose legislation or take positions or make recommendations on legislative proposals or issues. Contributing CRS staff include Patricia Moloney Figliola, (continued...)
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

Entries are in chronological order.\textsuperscript{32} The statutes discussed include only those for which CRS identified specific proposals to revise them from various observers and in public sources.\textsuperscript{33} It does not include proposals for new provisions of federal law that were not identified explicitly as revisions of current named statutes.

One example is the recommendations for statutory language on data-breach notification in the \textit{White House Proposal} and the \textit{Task Force Report}. Neither those two documents, nor the bills on the issue that have been introduced in the 112\textsuperscript{th} Congress,\textsuperscript{34} specify named statutes to be revised. One of those bills, S. 1151, would revise 18 U.S.C. Chapter 47 (Fraud and False Statements) by adding a new section at the end, but that provision does not modify any named statute specified either in the bill or in the U.S. Code. It is therefore not included in the discussion below. However, the bill would also revise 18 U.S.C. §1030, which was added by the “Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,” so that provision is discussed.

Another example is bills with provisions clearly related to a named statute, but that do not explicitly modify that statute. One example from the 111\textsuperscript{th} Congress is H.R. 5590, which had cybersecurity provisions that might be interpreted as modifications to the HSA but were not cited as such. Such provisions are not discussed in this report because their effects on specific statutes could not be determined with certainty.

The approach taken in this report of focusing on statutes by their popular names is useful in many cases, but it has some significant limitations, particularly with respect to the U.S. Code. Some laws, such as the USA Patriot Act of 2001 (see \textbf{Table 2}), may be classified across many titles and sections,\textsuperscript{35} which may make analysis more challenging. Fortunately, that did not prove to be a significant concern for this report.

However, lack of correspondence between named laws and proposed modification of provisions in the U.S. Code, described above, may in some cases result in significant gaps in coverage of relevant provisions of law relating to cybersecurity by an approach such as the one taken here. Therefore, the analysis presented here should not be regarded as complete.

\textsuperscript{32} The order is by date of enactment of the earliest relevant statute, as assessed by CRS. This organization, rather than alternatives such as by topic or U.S. Code title, was chosen because it provides the best view of the evolution of legislation in this area.
\textsuperscript{33} Sources are cited where they could be specifically identified.
\textsuperscript{34} See footnote 21.
\textsuperscript{35} This act was classified to 15 titles.
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

Posse Comitatus Act of 1879

Ch. 263, 20 Stat. 152.
18 U.S.C. §1385.36

Major Relevant Provisions

- Restricts the use of military forces in civilian law enforcement within the United States, unless it is within a federal government facility.37
- Courts have ruled that violations of the act occur when civilian law enforcement makes “direct active use” of military investigators, when use of the military pervades the activities of the civilian officials, or when the military is used so as to subject citizens to military power that is regulatory, prescriptive, or compulsory in nature.

Possible Updates

- Some observers claim that the act prevents the military from cooperating on cybersecurity with civil agencies that may lack the resident expertise and capabilities of the military and DOD.38 In addition, it may sometimes be difficult to distinguish a criminal cyber attack from one involving national defense, especially if the attack is on a component of critical infrastructure.
- Some have therefore proposed that the act be amended to clarify when U.S. military can operate domestically regarding cyber threats to such infrastructure, most of which is privately owned. Others maintain that no revision is needed because the President has the authority under current law to direct the military to support civil authorities in the event of a domestic disaster.
- A memorandum of agreement signed between DHS and DOD may increase the likelihood that the military would play a significant role in responding to a major cyber attack on U.S. information networks.39 However, some argue that the defense of U.S. information systems should be solely the purview of civilian agencies such as DHS and the FBI, because involvement of the military creates unacceptable privacy and civil liberties concerns.

36 Prepared by Catherine A. Theohary, Analyst in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844).
37 For further discussion, see CRS Report RS22266, The Use of Federal Troops for Disaster Assistance: Legal Issues, by Jennifer K. Elsea and R. Chuck Mason.
39 Department of Homeland Security and Department of Defense, “Regarding Cybersecurity.” The MOA provides terms for sharing of personnel, equipment, and facilities by the two agencies to improve planning, capabilities, and mission activities in national cybersecurity efforts.
Antitrust Laws and Section 5 of the Federal Trade Commission Act

Sherman Antitrust Act

Ch. 647, 26 Stat. 209.

Wilson Tariff Act

Ch. 349, §73, 28 Stat. 570.

Clayton Act


Section 5 of the Federal Trade Commission Act (FTC Act)

Ch. 311, §5, 38 Stat. 719.

When referred to in statute, the term “antitrust laws” generally means the three laws listed in 15 U.S.C. §12(a), which are the first three statutes listed above. Also frequently included in the list of antitrust laws is Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices. Section 5 is included because courts have found that unfair competition includes, at the least, activity that would violate the Sherman or Clayton Acts.41

Major Relevant Provisions

• The antitrust laws as well as Section 5 of the FTC Act are a collection of statutes that forbid combinations or agreements that unreasonably restrain trade.42 Whenever competitors in a given market share information, antitrust concerns may be raised due to the risk of collusion among competitors.43

Possible Updates

Information sharing agreements between private corporations may be subject to antitrust scrutiny, because the sharing of information among competitors could create opportunities for collaboration with the goal of restraining trade.44 However, information sharing agreements to

40 Prepared by Kathleen Ann Ruane, Legislative Attorney (kruane@crs.loc.gov, 7-9135).
44 Ibid.
combat cybersecurity may be in compliance with antitrust principles so long as their goals are to combat cyber threats rather than restrain competition.45

Some may argue that in order to develop effective and efficient information sharing agreements to combat cybersecurity threats, an explicit exemption from the antitrust laws for these agreements is necessary. Congress has previously proposed such an exemption. For example, H.R. 2435 (107th Congress) would have granted an express exemption from the antitrust laws and from Section 5 of the FTC Act to persons making and implementing agreements entered into solely for the purpose of “facilitating the correction or avoidance of a cyber security-related problem or communication of or disclosing information to help correct or avoid the effects of a cyber security-related problem.” Such an exemption, if enacted by Congress, would allow market participants to engage in information sharing for the purposes of combating cybersecurity threats without concern for implicating the antitrust laws. In the 112th Congress, the Task Force Report states that an antitrust exemption might be required.46

Others may argue that the antitrust laws are flexible in nature, particularly as they relate to information sharing agreements, and the laws are flexibly applied by the agencies of jurisdiction.47 This flexible nature may obviate the need for express exemptions from the application of the laws, while keeping the antitrust agencies involved in and aware of the information sharing agreements companies are making.48 The agencies have expressed a view that if competitors are collaborating for reasons that do not restrain trade or hamper competition, and safeguards are in place to prevent such restraint, the antitrust laws should not hinder such collaboration.49 The Department of Justice (DOJ) currently allows companies wishing to create information sharing arrangements for permissible and procompetitive purposes to submit their plans for collaboration to the agency.50 The agency then reviews the plans and, if the plans are approved, issues what is known as a business review letter.51 The business review letter will generally state that DOJ does not intend to enforce the antitrust laws against the proposed collaboration. DOJ has issued business review letters to companies who have developed plans to share information to combat cybersecurity threats.52

45 Ibid. (noting that many collaborations among competitors are “not only benign, but procompetitive”).
46 House Republican Cybersecurity Task Force, Recommendations, p. 11.
48 See Federal Trade Commission and Department of Justice, Antitrust Guidelines.
49 Ibid.
50 28 C.F.R. §50.6.
51 Federal Trade Commission and Department of Justice, Antitrust Guidelines.
National Institute of Standards and Technology Act

Ch. 872, 31 Stat. 1449.

Major Relevant Provisions

The original act gave the agency responsibilities relating to technical standards. Later amendments added more generally relevant provisions and, more specifically,

- Identified relevant research topics, among them computer and telecommunication systems, including information security and control systems.53
- Established a computer standards program at the National Institute of Standards and Technology (NIST).54

Possible Updates

Despite NIST’s current authority to conduct research on computers and information security, some concerns have been raised about whether those activities should be enhanced in light of the evolving threat environment for cybersecurity. In the 111th Congress, H.R. 4061, which was passed by the House, would have required NIST to conduct intramural research on identity management and the security of information systems, networks, and industrial control systems. A similar bill, H.R. 2096, is being considered by the 112th Congress.

Federal Power Act

Ch. 285, 41 Stat. 1063.
16 U.S.C. §791a et seq., §824 et seq.55

Major Relevant Provisions

- Established the Federal Energy Regulatory Commission (FERC) and gave it regulatory authority over interstate sale and transmission of electric power.

Possible Updates

Concerns about the vulnerability of the electric grid to cyber attack have increased substantially over the last several years.56 Although the Energy Policy Act of 2005 (P.L. 109-58) gave FERC

---

53 15 U.S.C. §272, as amended by the Technology Competitiveness Act, Subtitle B of Title V of P.L. 100-418, the Omnibus Trade and Competitiveness Act of 1988, which also changed the name of the agency from the National Bureau of Standards to the National Institute of Standards and Technology, and changed the name of the act to the National Institute of Standards and Technology Act.


55 The law was originally enacted in 1920 as the Federal Water Power Act but was renamed the Federal Power Act in 1935 (49 Stat. 863, 16 U.S.C. §791a).

56 See, for example, H.Rept. 111-493, S.Rept. 111-331.
responsibility for developing reliability standards for power systems, limitations to that authority and to the usefulness of the standards-development process to respond effectively to rapidly emerging cybersecurity threats have raised concerns about the need for enhancing FERC’s authority to address those threats, especially in light of the development of smart-grid technology.\textsuperscript{57} Several bills were introduced in the 111\textsuperscript{th} Congress (H.R. 2165, H.R. 2195, H.R. 5026, S. 946, S. 1462) in response. H.R. 5026, which was passed by the House, would have expanded FERC’s jurisdiction over electric infrastructure and authorized FERC to order actions by relevant entities in response to threats to cybersecurity. In the 112\textsuperscript{th} Congress, S. 1342 would also provide expanded cybersecurity authorities to FERC, and H.R. 668 would give FERC emergency authorities in response to events causing large-scale disruptions of the electric grid.

**Communications Act of 1934**

Ch. 652, 48 Stat. 1064.

47 U.S.C. §151 et seq.\textsuperscript{58}

**Major Relevant Provisions**

- Established the Federal Communications Commission (FCC) and gave it regulatory authority over both domestic and international commercial wired and wireless communications.

- Provides the President with authority in a national emergency to control “any or all stations or devices capable of emitting electromagnetic radiations,” and in case of war or threat of war, to close “any facility or station for wire communication” (Sec. 706 of the act, 47 U.S.C. §606).

**Possible Updates**

Some observers have proposed that the act should be revised to give the FCC more of a role in cybersecurity, especially given the growing merging of information and communications technology (ICT) and their increasing importance in the U.S. economy. In fact, a number of other countries have more unified governance of ICT than the United States.\textsuperscript{59}

Some controversy exists about whether the Section 706 authorities described above permit the President to shut down Internet communications during a war or national emergency, a power that has sometimes been referred to as the “Internet kill switch.”\textsuperscript{60} However, there does not appear to be a consensus about whether in fact such additional authority is needed, or, if it is not, whether additional legislation is needed to clarify and delimit it.

That debate became acute during Senate consideration of S. 773 and S. 3480 in the 111\textsuperscript{th} Congress. Those bills would have authorized emergency measures by the President if the


\textsuperscript{58} See also “Communications Decency Act of 1996.”


\textsuperscript{60} See also CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John Rollins.
operation of critical infrastructure were threatened by cyber attack. A similar provision has been proposed in S. 413 in the 112th Congress.61 This bill also contains a provision that would expressly deny the federal government of any authority to “shut down the Internet.”

National Security Act of 1947

Ch. 343, 61 Stat. 495
50 U.S.C. 401 et seq.

Major Relevant Provisions

- Provided the basis for the modern organization of U.S. defense and national security by reorganizing military and intelligence functions in the federal government.
- Created the National Security Council, the Central Intelligence Agency, and the position of Secretary of Defense.
- Established procedures for access to classified information.

Possible Updates

A broad consensus exists that a significant barrier to improving cybersecurity is limitations on sharing of information, including classified information, about cyber-threats and attacks.62 H.R. 3523 would address that concern by amending the act to facilitate sharing of intelligence information relating to cybersecurity between federal intelligence entities and private-sector providers of cybersecurity services, and to facilitate the identification and sharing of threat information by providers. The bill also includes provisions for protection from liability for entities sharing information and exemption from disclosure of that information under the “Freedom of Information Act (FOIA).”

---

61 S. 413 is largely identical to S. 3480. Both would provide the authority for the emergency measures through a revision of the Homeland Security Act, not the Communications Act. In addition, they would assign the authority to implement Sec. 706 to the head of a White House office to be created by the bills. The provision in S. 773 was not presented as a revision to a specified law.

62 For example, the Task Force Report states, “There is widespread agreement that greater sharing of information is needed within industries, among industries, and between government and industry in order to improve cybersecurity and to prevent and respond to rapidly changing threats. For example, through intelligence collection, the federal government has insights and capabilities that many times are classified but would be useful to help defend private companies from cybersecurity attacks” (House Republican Cybersecurity Task Force, Recommendations, p. 10).
U.S. Information and Educational Exchange Act of 1948 (Smith-Mundt Act)

Ch. 36, 62 Stat. 6.
22 U.S.C. §1431 et seq. 63

Major Relevant Provisions

- Restricts the State Department from disseminating public diplomacy information domestically and limits its authority to communicate with the American public in general (22 U.S.C. §1461-1a). 64 The domestic dissemination provision originally applied to the now defunct U.S. Information Agency (USIA), which was abolished and its functions transferred to the Secretary of State by P.L. 105-277 (22 U.S.C. §6532). 65

Possible Updates

Critics maintain that the law is a Cold War relic intended only to restrict the USIA, which no longer exists, from propagandizing Americans with public diplomacy and information materials that were intended for a foreign audience. Those critics argue that the restrictions were created before the advent of the Internet, and the provisions create an obsolete barrier that serves only to prevent the State Department from communicating effectively. Some have also argued that the law has been interpreted to prohibit the military from conducting information operations in cyberspace, as some of those activities could be considered propaganda that could reach U.S. citizens, since the United States does not restrict Internet access according to territorial boundaries.

Yearly appropriations bills for both the State Department and Department of Defense include restrictions on use of funds for “propaganda” activities, although the word “propaganda” is not defined. In the 111th Congress, H.R. 5729 would have removed the so-called “firewall” between domestic and foreign audiences by explicitly authorizing the Department of State to disseminate information through the Internet and information media, stating that the resolution shall “not be construed to prohibit the Department from engaging in any medium of information on a presumption that a U.S. domestic audience may be exposed to program material.” However, this provision would have applied only to the State Department; it would not have included DOD or other federal departments or agencies.

63 Prepared by Catherine A. Theohary, Analyst in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844).

64 This restriction was added by the Foreign Relations Authorization Act, Fiscal Years 1986 and 1987 (P.L. 99-93, 99 Stat. 431) and was not part of the original act.

65 For discussion, see CRS Report R40989, U.S. Public Diplomacy: Background and Current Issues, by Kennon H. Nakamura and Matthew C. Weed.
State Department Basic Authorities Act of 1956

Ch. 841, 70 Stat. 890.

Major Relevant Provisions

- Specifies the organization of the Department of State, including the positions of coordinator for counterterrorism and for HIV/AIDS response.

Possible Updates

As the Internet becomes increasingly international, concerns have been raised about the development and coordination of international efforts in cybersecurity by the United States. In the 111th Congress, S. 3193 would have addressed those concerns by establishing a coordinator for cyberspace and cybersecurity issues within the Department of State. S. 1426 in the 112th Congress contains a similar provision.

Freedom of Information Act (FOIA)

P.L. 89-487, 80 Stat. 250.
5 U.S.C. §552. 67

Major Relevant Provisions

- Enables any person to access—without explanation or justification—existing, identifiable, unpublished executive-branch agency records, unless the material falls within any of FOIA’s nine categories of exemption from disclosure.

Possible Updates

Sharing of cybersecurity information between the federal government and nonfederal entities is widely considered to be an essential need, especially with respect to the protection of critical infrastructure (CI). However, attempts to encourage the private sector to share sensitive CI information with the federal government have, at times, been met with concerns that such records could be subject to public release under FOIA, resulting in potential economic or other harm to the source.

Among the nine exemptions that permit agencies to withhold applicable records are three that may particularly apply to cybersecurity information:


67 Prepared by Wendy R. Ginsberg, Analyst in Government Organization and Management (wginsberg@crs.loc.gov, 7-3933).
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

- **Exemption 1**: information properly classified for national defense or foreign policy purposes as secret under criteria established by an executive order.

- **Exemption 3**: data specifically exempted from disclosure by a statute other than FOIA if that statute meets criteria laid out in FOIA. ⁶⁸

- **Exemption 4**: trade secrets and commercial or financial information obtained from a person that is privileged or confidential. ⁶⁹

An example of Exemption 3 is Sec. 214 of the HSA (see p. 30), which exempts information about the security of critical infrastructure and protected systems that is voluntarily submitted to an agency covered under the act, provided that the entity that supplies the information expressly requests the exemption concurrently.

Despite these existing protections, some private-sector entities may still have concerns about public release of sensitive records—that existing laws may not be specific enough to protect particular types of records, or they may be too narrow to protect all records of concern. The White House Proposal would address such concerns by applying Exemption 3 to any lawfully obtained information provided to DHS for cybersecurity purposes. ⁷⁰ The Task Force Report also suggests that a FOIA exemption may be needed, ⁷¹ and the draft bill being considered by the House Committee on Homeland Security, as well as H.R. 3523, would provide such a FOIA exemption, although none of those proposals would directly modify the statute. Adding such broad exemptions to FOIA, however, could nevertheless prompt concerns about decreases in federal transparency.

---

⁶⁸ The statute must require that the data be withheld from the public in such a manner as to leave no discretion on the issue, establish particular criteria for withholding information or refer to particular types of matters to be withheld, or specifically cite the exemption if enacted after October 28, 2009, the date of enactment of the OPEN FOIA Act of 2009, P.L. 111–83. These exemptions are also called “b(3) exemptions” because they are created pursuant to 5 U.S.C. §552(b)(3).


⁷¹ Specifically, it states, “information sharing within existing structures can be improved through limited safe harbors when private sector entities voluntarily disclose threat, vulnerability, or incident information to the federal government or ask for advice or assistance to help increase protections on their own systems. These protections would need to address concerns about antitrust issues, liability, an exemption from the Freedom of Information Act (FOIA), protection from public disclosure, protection from regulatory use by government, and whether or not a private entity is operating as an agent of the government. However, the protection of personal privacy should be at the forefront of any limited legal protection proposal” (House Republican Cybersecurity Task Force, Recommendations, p. 11).
Omnibus Crime Control and Safe Streets Act of 1968

42 USC Chapter 46, §§3701 to 3797ee-1.

Major Relevant Provisions

- Title I established federal grant programs and other forms of assistance to state and local law enforcement.
- Title III is a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both activities in general terms but that also permitted federal and state law enforcement officers to use them under strict limitations.\(^{72}\)

Possible Updates

The incidence of cybercrime has increased dramatically over the last decade.\(^{73}\) State and local law enforcement agencies play an important role in combating cybercrime, but concerns have been raised about their abilities to invest sufficient resources in enforcement activities. In the 111th Congress, H.R. 1292 would have added a program for law enforcement grants to state and local criminal justice agencies and relevant nonprofit organizations to combat “white collar crime,” including cybercrime.

Racketeer Influenced and Corrupt Organizations Act (RICO)

P.L. 91-452, 84 Stat. 941.

Major Relevant Provisions

- Enlarges the civil and criminal consequences of a list of state and federal crimes when committed in a way characteristic of the conduct of organized crime (racketeering).\(^{74}\)

Possible Updates

The Task Force Report recommends that Congress change RICO “to include computer fraud within the definition of racketeering.”\(^{75}\)

---

\(^{72}\) These provisions, along with possible updates, are discussed under “Electronic Communications Privacy Act of 1986.”

\(^{73}\) There is no uniform definition of “cybercrime.” Furthermore, no definitive statistics on cybercrime appear to be publicly available. However, the public/private Internet Crime Complaint Center referred 25 times as many of the complaints it received to law enforcement agencies in 2010 (121,710) as in 2001 (4,810) (Internet Crime Complaint Center, 2010 Internet Crime Report, 2011, http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf).

\(^{74}\) For details, CRS Report 96-950, RICO: A Brief Sketch, by Charles Doyle.

Federal Advisory Committee Act (FACA)

5 U.S.C. App., §§1-16.

Major Relevant Provisions

- Specifies the circumstances under which a federal advisory committee can be established, and its responsibilities and limitations.
- Requires that meetings of such committees be open to the public and that records be available for public inspection.76

Possible Updates

The act has been criticized as potentially impeding the full development of public/private partnerships in cybersecurity, particularly with respect to impeding private-sector communications and input on policy.77 While Sec. 871 of the HSA provides the Secretary of Homeland Security with the power to establish advisory committees that are exempt from the requirements of the act, it is possible that additional exemption authority would be helpful. Any such potential benefits might, however, need to be weighed against the impact of such authority on the public’s ability to participate in and access the records of affected advisory committees. The draft bill being considered by the House Committee on Homeland Security78 would exempt the organization created by the bill from requirements of the act.

Privacy Act of 1974


Major Relevant Provisions

- Limits the disclosure of personally identifiable information (PII) held by federal agencies.
- Requires agencies to provide access to persons with agency records containing information on them.
- Established a code of fair information practices for collection, management, and dissemination of records by agencies, including requirements for security and confidentiality of records.

---

76 For more information, see CRS Report R40520, Federal Advisory Committees: An Overview, by Wendy Ginsberg.
78 House Committee on Homeland Security, “Hearing on Draft Legislative Proposal on Cybersecurity.”
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

Possible Updates

Some observers argue that the act should be revised to clarify, in the context of cybersecurity, what is considered PII and how it can be used, such as by explicitly permitting the sharing among federal agencies—or with appropriate third parties such as owners and operators of critical infrastructure—of certain information, such as a computer’s Internet (IP) address, in examinations of threats, vulnerabilities, and attacks. The act contains some exemptions, such as for law enforcement activities (5 U.S.C. §552a(b)(7)) and duties of the Comptroller General (5 U.S.C. §552a(b)(10)), but none relating specifically to cybersecurity. However, other observers may argue that the provisions in the act are sufficient to permit necessary cybersecurity activities, and that revising the act to provide additional authorities relating to cybersecurity could compromise the protections provided by the act. 79 In the 112th Congress, H.R. 1732 would revise the act to take changes in information technology into account, but does not specifically address information relating to cybersecurity.

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984


Major Relevant Provisions

As amended,80

• Provides criminal penalties, including asset forfeiture, for unauthorized access and wrongful use of computers and networks of the federal government or financial institutions, or in interstate or foreign commerce or communication;
• Specifies wrongful use as obtaining protected information, damaging or threatening to damage a computer, using the computer to commit fraud, trafficking in stolen computer passwords, and espionage;
• Criminalized electronic trespassing on and exceeding authorized access to federal government computers; and
• Created a statutory exemption for intelligence and law enforcement activities.81

80 The Computer Fraud and Abuse Act of 1986 (P.L. 99-474, 100 Stat. 1213) expanded the scope of the original act. For government computers, it criminalized electronic trespassing, exceeding authorized access, and destroying information. It also criminalized trafficking in stolen computer passwords and created a statutory exemption for intelligence and law enforcement activities.
81 For more information, see CRS Report 97-1025, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, by Charles Doyle.
Possible Update

The White House Proposal would add penalties for damaging certain critical infrastructure computers, increase penalties for most violations of the act, modify its conspiracy and forfeiture provisions, and make felony violation of the act a racketeering predicate offense. In the 112th Congress, S. 890 would enlarge the scope of the password trafficking offense by removing the requirement that the computer affect interstate commerce or be used by the United States, as would the White House Proposal. S. 1151 would also make several changes similar to but not as extensive as those in the Administration proposal. The Task Force Report recommends that the act be broadened to cover critical infrastructure systems, and possibly all private-sector computers, with increased criminal penalties. Provisions should be focused narrowly enough to avoid creating unintended liability for legitimate activities.

Electronic Communications Privacy Act of 1986 (ECPA)


Major Relevant Provisions

- Attempts to strike a balance between the fundamental privacy rights of citizens and the legitimate needs of law enforcement with respect to data shared or stored in various types of electronic and telecommunications services. Since the act was passed the Internet and associated technologies have expanded exponentially. The act consists of three parts:
  - A revised Title III of the “Omnibus Crime Control and Safe Streets Act of 1968” (also known as “Title III” or the “Wiretap Act”) prohibits the interception of wire, oral, or electronic communications unless an exception to the general rule applies. Unless otherwise provided, prohibits wiretapping.

84 Prepared by Gina Stevens, Legislative Attorney (gstevens@crs.loc.gov, 7-2581).

In 1986, when ECPA was passed, the Internet consisted of a few thousand computers. The network was run by the U.S. government for research and education purposes, and commercial activity was forbidden. There were no web pages, because the web had not been invented. Google would not be founded for another decade. Twitter would not be founded for another two decades. Mark Zuckerberg, who would grow up to start Facebook, was two years old. In talking about advances in computing, people often focus on the equipment. Certainly the advances in computing equipment since 1986 have been spectacular. Compared to the high-end supercomputers of 1986, today’s mobile phones have more memory, more computing horsepower, and a better network connection not to mention a vastly lower price.

and electronic eavesdropping; possession of wiretapping or electronic eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice.88

- The Stored Communications Act (SCA)89 prohibits unlawful access to stored communications.90

- The Pen Register and Trap and Trace statute governing the installation and use of trap and trace devices and pen registers,91 proscribing unlawful use of a pen register or a trap and trace device.92

- Establishes rules that law enforcement must follow before they can access data stored by service providers. Depending on the type of customer information involved and the type of service being provided, the authorization law enforcement must obtain in order to require disclosure by a third party will range from a simple subpoena to a search warrant based on probable cause.

**Possible Updates**

ECPA reform efforts focus on crafting a legal structure that is up-to-date, can be effectively applied to modern technology, and that protects users’ reasonable expectations of privacy. ECPA is viewed by many stakeholders as unwieldy, complex, and difficult for judges to apply.93 Cloud computing94 poses particular challenges to the ECPA framework. For example, when law enforcement officials seek data or files stored in the cloud, such as web-based e-mail applications or online word processing services, the privacy standard that is applied is often lower than the standard that applies when law enforcement officials seek the same data stored on an individual’s personal or business hard drive.95

An ECPA reform advocacy coalition has advanced the following principles:

---

91 18 U.S.C. §§3121-3126. A trap and trace device identifies the source of incoming calls, and a pen register indicates the numbers called from a particular phone.
94 “Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers, while freeing them from the burden and costs of maintaining the underlying infrastructure. Examples of cloud computing include web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer” (Government Accountability Office, Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing, GAO-10-513, May 2010, http://www.gao.gov/new.items/d10513.pdf).
95 House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, *ECPA Reform and the Revolution in Cloud Computing* (statement of Michael Hintze, Associate General Counsel, Microsoft Corp.).
A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public, but only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider’s access to or use of the communications in its normal business operations.

A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device, but only with a warrant issued based on a showing of probable cause.

A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, e-mail to and from information or other data currently covered by the authority for pen registers and trap and trace devices, but only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).

Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All nonparticularized requests must be subject to judicial approval.96

The Task Force Report recommends changes to laws governing the protection of electronic communications to facilitate sharing of appropriate cybersecurity information, including the development of an anonymous reporting mechanism.97

Department of Defense Appropriations Act, 1987

10 U.S.C. §167.98

Major Relevant Provisions

- Provides specific authority to the U.S. Special Operations Command (USSOCOM) for the conduct of direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, civil affairs, and psychological operations; also counterterrorism, humanitarian assistance, theater search and rescue, and such other activities as may be specified by the President or the Secretary of Defense.


98 Prepared by John Rollins, Specialist in Terrorism and National Security (jrollins@crs.loc.gov, 7-5529).
Possible Update

In addition to the authority provided under this act, Title 10 of the U.S. Code provides inherent and specific authority to DOD to undertake the following activities:

- §113 provides that, subject to the direction of the President, the Secretary of Defense has authority, direction, and control over DOD;
- §164 provides specific authority for combatant commanders for the performance of missions assigned by the President or by the Secretary with the approval of the President.

Specific authorities for combatant commanders are provided in Title 10 to use force in self-defense and for mission accomplishment—including in the recently recognized information operations environment. In preparing for contingencies or military operations, DOD undertakes activities to lessen risks to U.S. interests, including discrete actions to prepare for and respond to a cyberwarfare-related incident.99

Some military activities are conducted clandestinely to conceal the nature of the operation and passively collect intelligence. Activities focused on influencing the governing of a foreign country are deemed covert actions100 and may not be conducted by members of the military absent a presidential finding and notification of the congressional intelligence committees.101

Some analysts suggest that in the cyber domain distinguishing between whether an action is or should be considered covert or clandestine is problematic, as an attacking adversary’s intent and location are often difficult to discern. Should this act be updated, reassessing DOD’s authorities in light of its unique intelligence capabilities may assist in responding to and conducting offensive cyber attacks.

High Performance Computing Act of 1991

15 U.S.C. Chapter 81.102

Major Relevant Provisions

- Establishes a federal high-performance computing program and requires that it address security needs.

---

100 50 U.S.C. §413b(e) defines a covert action as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include … activities the primary purpose of which is to acquire intelligence … [or] traditional military activities or routine support to such activities.”
101 For an explanation and analysis of issues relating to covert and clandestine activities see CRS Report RL33715, Covert Action: Legislative Background and Possible Policy Questions, by Alfred Cumming and Richard A. Best Jr.
102 Parts of the chapter have also been given other popular names: the Next Generation Internet Research Act of 1998 (P.L. 105-305), and the Department of Energy High-End Computing Revitalization Act of 2004.
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

- Requires that the program provide for interagency coordination and that an annual report on implementation be submitted to Congress.
- Requires NIST to establish security and privacy standards in high-performance computing for federal systems.

Possible Updates

This act established the Networking and Information Technology Research and Development (NITRD) Program, which produces the required annual report. However, concerns have been raised that the program does not yield sufficient strategic planning and does not sufficiently stress cybersecurity research and development (R&D). In the 111th Congress, H.R. 2020 would have addressed that concern by requiring a five-year strategic plan with three-year reviewing cycle. It would also have added a research goal of increasing understanding “of the scientific principles of cyber-physical systems” and improving methods for designing, developing, and operating such systems with high reliability, safety, and security. S. 773 would have required NIST to develop cybersecurity standards and metrics for computer networks and user interfaces.

Communications Assistance for Law Enforcement Act of 1994 (CALEA)

47 U.S.C. §1001 et seq.103

Major Relevant Provisions

- Requires telecommunications carriers to assist law enforcement in performing electronic surveillance on their digital networks pursuant to court orders or other lawful authorization.
- Directs the telecommunications industry to design, develop, and deploy solutions that meet requirements for carriers to support authorized electronic surveillance, including unobtrusive isolation of communications and call-identifying information for a target and provision of that information to law enforcement, in a manner that does not compromise the privacy and security of other communications.

Possible Updates

Some government and industry observers believe that CALEA should be revised to improve its effectiveness in addressing cybersecurity concerns. Among the concerns expressed are whether the act is the best mechanism for collecting information transmitted via the Internet, whether reassessment is needed of which private-sector entities the act covers and which government entities should be involved in enforcement and oversight, and what the role of industry should be in the development of the technologies and standards used to implement the provisions of the act.

103 Prepared by Patricia Moloney Figliola, Specialist in Internet and Telecommunications Policy (pfigliola@crs.loc.gov, 7-2508).
The Task Force Report recommends changes to laws governing the protection of electronic communications to facilitate sharing of appropriate cybersecurity information, including the development of an anonymous reporting mechanism.  

Communications Decency Act of 1996

P.L. 104-104 (Title V), 110 Stat. 133.

Major Relevant Provisions

- Intended to regulate indecency and obscenity on telecommunications systems, including the Internet. Although much of the law is targeted at lewd or pornographic material, particularly when shown to children under the age of 18, the obscenity and harassment provisions could also be interpreted as applying to graphic, violent terrorist propaganda or incendiary language.
- Section 230(c)(1) asserts that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information.” This has been interpreted to absolve Internet service providers and certain web-based services of responsibility for third-party content residing on those networks or websites.

Possible Updates

Some argue that certain Internet content, such as terrorist chat rooms or propaganda websites, presents a national security or operational threat that is not represented within the Communications Decency Act. Further, should such material be deemed as “indecent,” the law does not give federal agencies the authority to require that the Internet service providers hosting the content to take it offline.

These critics maintain that the law should be revised to compel ISPs and web administrators to dismantle sites containing information that could be used to incite harm against the United States. A possible revision could be similar to the “take down and put back” provision in the Digital Millennium Copyright Act, 112 Stat. 2860, P.L. 105-304 which amended title 17 of the U.S. Code to hold a service liable for publishing material that is defamatory or infringes upon a third party copyright.

Others maintain that such a revision is counter to the spirit of free, open exchange of information that is characterized by the Internet and may be a First Amendment violation. Some have also expressed concerns that the intelligence value gained by preserving and monitoring the sites outweighs the potential threat risk.

105 Prepared by Catherine A. Theohary, Analyst in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844). These provisions are codified to Chapter 5 of Title 47, the “Communications Act of 1934.” Codification of the various provisions of this act is complex. See 47 U.S.C. §609 nt. for details.
106 See CRS Report R41499, The Communications Decency Act: Section 230(c)(1) and Online Intermediary Liability, by Kathleen Ann Ruane and Julia Tamulis.
Clinger-Cohen Act (Information Technology Management Reform Act) of 1996

P.L. 104-106 (Divisions D and E), 110 Stat. 642.
40 U.S.C. §11101 et seq. 107

Major Relevant Provisions

• Gave agency heads authority to acquire IT and required them to ensure the adequacy of agency information security policies.
• Established the position of agency Chief Information Officer (CIO), responsible for assisting agency heads in IT acquisition and management.
• Requires the Office of Management and Budget (OMB) to oversee major information technology (IT) acquisitions.
• Requires OMB to promulgate, in consultation with the Secretary of Homeland Security, compulsory federal computer standards based on those developed by the National Institute of Standards and Technology (NIST). 108
• Exempts national security systems from most provisions.

Possible Update

With the increasing globalization of the IT hardware and software industries, concerns have been growing among cybersecurity experts about potential vulnerabilities at various points along the supply chain for IT products. H.R. 1136, introduced in the 112th Congress, would address such concerns with respect to federal acquisition of IT products and services by requiring vendors to meet security requirements to be developed by OMB, and also requiring vulnerability assessments by agencies. S. 413 (similar to S. 3480 in the 111th Congress) and the White House Proposal would return the authority for promulgating standards for federal systems to the Secretary of Commerce. 109

Congress and the executive branch have debated the limits of the authority and jurisdiction of CIOs since their establishment. In the private sector, CIOs may often serve as the senior IT decisionmaker. In federal agencies, in contrast, CIOs do not have budgetary control or authority over IT resources. 110 As part of a plan to reform federal IT management, 111 the Obama

---

107 Prepared by Wendy R. Ginsberg, Analyst in Government Organization and Management (wginsberg@crs.loc.gov, 7-3933), and Eric A. Fischer. The two divisions, originally known as the Federal Acquisition Reform Act and the Information Technology Management Reform Act, were renamed as the Clinger-Cohen Act by P.L. 104-208 and reclassified into 40 U.S.C. Subtitle III by P.L. 107-217 (see 40 U.S.C. §101 nt.).

108 The Clinger-Cohen Act originally gave this promulgation authority to the Secretary of Commerce, while providing the President authority to disapprove or modify such standards, and gave the Secretary authority to waive the standards in specific cases to avoid adverse financial or mission-related impacts. The “Federal Information Security Management Act of 2002 (FISMA)”, enacted as part of the Homeland Security Act, transferred that authority to OMB.

109 See the discussion of FISMA, p. 32.

110 They do have authority under FISMA to ensure compliance with that law’s information security requirements (44 U.S.C. §3544). Some agency CIOs also have statutory authority in addition to that provided by Clinger-Cohen and FISMA. For example, the CIO of the intelligence community has procurement approval authority for IT (50 U.S.C. (continued...))
Administration has indicated its intention to change the role of CIOs “away from just policymaking and infrastructure maintenance, to encompass true portfolio management for all IT,” including information security.\textsuperscript{112} The \textit{White House Proposal} does not include any provisions related to that proposed change, but additional legislative authority may be required for such a change to be fully implemented.

The Obama Administration also appointed a federal chief information officer and a federal chief technology officer (CTO), positions first created in the George W. Bush Administration, where the OMB deputy director of management also served as federal CIO. In the 111\textsuperscript{th} Congress, H.R. 1910 and H.R. 5136, and H.R. 1136 in the 112\textsuperscript{th} Congress, contain provisions to establish a statutory basis for the CTO position, not, however, explicitly as amendments to the Clinger-Cohen Act.\textsuperscript{113} Some proposals in previous Congresses would also have established the federal CIO position in law.\textsuperscript{114}

\section*{Identity Theft and Assumption Deterrence Act of 1998}

P.L. 105-318, 112 Stat. 3007.\textsuperscript{115} 18 U.S.C. \S\S 1028.\textsuperscript{115}

\begin{itemize}
\item Made identity theft a federal crime.
\item Provided penalties for individuals who either committed or attempted to commit identity theft.
\item Provided for forfeiture of property used or intended to be used in the fraud.
\item Directed the Federal Trade Commission (FTC) to record complaints of identity theft, provide victims with informational materials, and refer complaints to the appropriate consumer reporting and law enforcement agencies.\textsuperscript{116}
\end{itemize}

(...continued)


\textsuperscript{114} See, for example, CRS Report RL30914, \textit{Federal Chief Information Officer (CIO): Opportunities and Challenges}, by Jeffrey W. Seifert.

\textsuperscript{115} Prepared by Kristin M. Finklea, Coordinator, Analyst in Domestic Security (kfinklea@crs.loc.gov, 7-6259). See 18 U.S.C. \S\S 1001 nt. for classification details.

Possible Updates

See “Identity Theft Penalty Enhancement Act” below.

**Homeland Security Act of 2002 (HSA)**

6 U.S.C. §§121-195c, 441-444, and 481-486.\(^{117}\)

**Major Relevant Provisions**

- Transferred some functions relating to the protection of information infrastructure from other agencies to the Department of Homeland Security (DHS).\(^ {118}\)
- Requires DHS to provide state and local governments and private entities with threat and vulnerability information, crisis-management support, and technical assistance relating to recovery plans for critical information systems.
- Permits the Secretary of Homeland Security to designate qualified technologies as subject to certain protections from liability in claims relating to their use in response to an act of terrorism.\(^ {119}\)
- Established mechanisms to facilitate information sharing among federal agencies and appropriate nonfederal government and critical-infrastructure personnel.\(^ {120}\)
- Authorized DHS to establish a system of volunteer experts (“Net Guard”) to assist local communities in responding to attacks on information and communications systems.
- Strengthened some criminal penalties relating to cybercrime.
- Created the Directorate of Science and Technology within DHS and assigned it broad R&D responsibilities, although responsibilities relating to cybersecurity R&D were not specifically described.

**Possible Updates**

Various concerns have been raised about the ways in which the act addressed cybersecurity, and a number of proposals have been made since its enactment to enhance the cybersecurity provisions. In the 111\(^{th}\) Congress, the most comprehensive legislative proposal was in S. 3480, which was reported out of the Senate Committee on Homeland Security and Governmental Affairs in the

---

\(^{117}\) For classification details, see 6 U.S.C. §101 nt.


\(^{119}\) This set of provisions (Subtitle G of Title VIII, 6 U.S.C. §§441-444) is called the SAFETY Act.

\(^{120}\) This set of provisions (Subtitle I of Title VIII, 6 U.S.C. §§481-486) is called the Homeland Security Information Sharing Act. Sec. 486 was added by P.L. 109-90 and provides some liability protections relating to actions involving information sharing and analysis centers.
111th Congress, and reintroduced in the 112th Congress as S. 413 with minor modifications. It would add provisions on cybersecurity that would

- establish a center for cybersecurity and communications within DHS;
- require coordination with the DHS Office of Infrastructure Protection and sector-specific agencies;
- establish the United States Computer Emergency Readiness Team (US-CERT) within the center;
- stipulate information-sharing procedures for federal agencies and other entities;
- establish a program within the center to provide assistance to the private sector;
- require the center to identify cyber vulnerabilities to critical infrastructure and establish requirements to address them;
- establish procedures for response to imminent cyber threats to critical infrastructure, enforcement of requirements, and protection of information; and
- require a risk-management strategy for security of the supply chain.

It would establish a cybersecurity R&D program in DHS and require coordination of those activities with other agencies and private entities. It would also establish a public/private-sector cybersecurity advisory council.

The White House Proposal would also substantially enhance DHS authority relating to cybersecurity. The proposal would differ in several ways from the approach taken by S. 413. Among other differences, it would provide enhanced authority to the DHS Secretary that S. 413 provides directly to a new center within the department. However, the White House Proposal would require the Secretary to establish a center with cybersecurity responsibilities for federal and critical infrastructure systems. It also does not codify the establishment of US-CERT, unlike S. 413, and does not provide the President with the authority to implement emergency actions in response to an imminent risk to critical infrastructure. It does, however, provide the DHS Secretary with authority to direct responses of federal agencies to cybersecurity threats or incidents.

Some other bills in the 111th Congress would also have revised the act. H.R. 6423, reintroduced as H.R. 174 in the 112th Congress, would establish a new office to develop, oversee, and enforce cybersecurity compliance for critical infrastructure sectors. H.R. 266, reintroduced as H.R. 76, would add a cybersecurity fellowship program for nonfederal officials to familiarize them with DHS cybersecurity activities. H.R. 4507 and H.R. 4842 would have added a cybersecurity training initiative for first responders and others. H.R. 2868 and S. 3599 would have added chemical-facility security measures, including cybersecurity, to the act.

In the 112th Congress, S. 1546 would add cybersecurity to the research topics covered by programs in the Science and Technology Directorate of DHS. A draft bill being considered by the

---

121 See also “Communications Act of 1934” above.
122 This center would presumably replace the federal incident center currently required under 44 U.S.C. 3546. The revision of the Federal Information Security Management Act of 2002 (FISMA) in the White House Proposal does not include the latter center.
House Committee on Homeland Security would revise the act to create a nongovernmental clearinghouse for sharing cybersecurity information between the private sector and the federal government, as recommended by the Task Force Report. It would also provide additional responsibilities and authorities to DHS for the protection of federal information systems and private-sector critical infrastructure (CI) systems, including the identification of sector-specific risks and standards for addressing them, information sharing with federal and nonfederal entities, cybersecurity research and development (R&D), and recruitment and retention of cybersecurity personnel.\(^{123}\)

### Federal Information Security Management Act of 2002 (FISMA)

P.L. 107-296 (Title X), 116 Stat. 2259.
P.L. 107-347 (Title III), 116 Stat. 2946.

#### Major Relevant Provisions

FISMA created a security framework for federal information systems, with an emphasis on risk management, and gave specific responsibilities to the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the heads, chief information officers (CIOs), chief information security officers (CISOs), and inspector generals (IGs) of federal agencies.\(^ {125}\)

- Required executive agencies to inventory major computer systems, identify and provide appropriate security protections, and develop, document, and implement agency-wide information security programs.
- Gave OMB responsibility for overseeing federal information-security policy and evaluating agency information-security programs, but exempted national security systems, except with respect to enforcement of accountability for meeting requirements and reporting to Congress.
- Revised the responsibilities of the Secretary of Commerce and NIST for information-system standards and transferred responsibility for promulgation of those standards from the Secretary of Commerce to OMB.\(^ {126}\)

---

\(^{123}\) House Committee on Homeland Security, “Hearing on Draft Legislative Proposal on Cybersecurity.”

\(^{124}\) FISMA was originally enacted as part of the Homeland Security Act. It was then reenacted by the E-government Act. Subchapter II is not in effect. The title 40 provision was originally enacted as part of the Clinger-Cohen Act (see p. 28), and the title 15 provisions are part of the NIST Act (see p. 13). See footnote 126 for more detail.


\(^{126}\) The standards-promulgation authority had been granted to the Secretary of Commerce under the Clinger-Cohen Act of 1996 (P.L. 104-106) but was transferred to the Director of OMB by the FISMA title in the HSA in 2002 (P.L. 107-296, Sec. 1002, 40 U.S.C. 11331). The version of the main Chapter 35 currently in effect (Subchapter III) was enacted by the FISMA title in the E-Government Act of 2002 (P.L. 107-347, Title III), which suspended Subchapter II, which had been revised by the HSA. That is not the case for 40 U.S.C. 11331, for which the P.L. 107-347 version would have retained the authority of the Secretary of Commerce to promulgate those standards as established in the Clinger-Cohen Act of 1996 (see p. 28), even though the E-Government Act was enacted after the HSA. Similarly, the revision to the NIST Act at 15 U.S.C. 278g-3 & 4 is that made by the HSA. The reason for this potentially confusing difference (continued...)
• Required that NIST cybersecurity standards be complementary with those
developed for national security systems, to the extent feasible.

• Required heads of federal agencies to provide security protections commensurate
with risk and to comply with applicable security standards. Specifically required
agencies using national security systems to provide security protections
commensurate with risk and in compliance with standards for such systems.

• Required senior agency officials to perform risk assessments, to determine and
implement necessary security controls in a cost-effective manner, and to evaluate
those controls periodically.

• Designated specific information-security responsibilities for agencies’ chief
information security officers, including agency-wide information-security
programs, policies, and procedures, and training of security and other personnel.

• Required designation of an information-security officer in each agency, security
awareness training, processes for remedial action to address deficiencies, and
procedures for handling security incidents and ensuring continuity of operations.

• Required annual agency reports to Congress, performance plans, and independent
evaluations of information security.

• Established a central federal incident center, overseen by OMB, to analyze
incidents and provide technical assistance relating to them, to inform agency
operators about current and potential threats and vulnerabilities, and to consult
with NIST, NSA, and other appropriate agencies about incidents.

• Gave responsibility for protection of mission-crucial systems in DOD and the
CIA to the Secretary of Defense and the DCI, respectively, and required the
Secretary of Defense to include compliance with the provisions above in
developing program strategies for the Defense Information Assurance Program

Possible Updates

A commonly expressed concern about FISMA is that it is awkward and inefficient in providing
adequate cybersecurity to government IT systems. The causes cited have varied but common
themes have included inadequate resources, a focus on procedure and reporting rather than
operational security, lack of widely accepted cybersecurity metrics, variations in agency
interpretation of the mandates in the act, and insufficient means to enforce compliance both
within and across agencies.127 Several legislative proposals in the 111th and 112th Congresses have

(...continued)

appears to be that (1) the effective date of HSA was later than that of the E-Government Act, and (2) HSA amended the
existing subchapter II of 44 U.S.C. Chapter 35; the E-Government Act explicitly suspended that subchapter. In
contrast, the revisions both laws made to the Paperwork Reduction Act, adding a subsection (c) to 44 U.S.C. §3505
(requiring inventories of federal information systems) were codified.

127 See, for example, S.Rept. 111-368, and House Subcommittee on Government Management, Organization, and
Procurement, The State of Federal Information Security, Committee on Oversight and Government Reform
CHRG-111hhrg57125.pdf. OMB has recently attempted to address some of the operational issues administratively by
delegating some responsibilities to DHS (Orszag and Schmidt, "Clarifying Cybersecurity Responsibilities and
(continued...)
included major revisions to the act. The proposals varied in detail, but several themes emerge from examination of them:

- Creation of a White House office with responsibility for cybersecurity;
- Transfer of responsibilities from OMB to a new cybersecurity center established in DHS and to the Secretary of Commerce;
- Revisions to agency responsibilities under the act, including continuous monitoring, use of metrics, and emphasis on risk-based rather than minimum security measures;
- Changes in reporting requirements;
- Specification of cybersecurity requirements for acquisitions and the IT supply chain; and
- Establishment of mechanisms for interagency collaboration on cybersecurity.

In the 111th Congress, H.R. 5136 passed in the House, and S. 3480 was reported out of the Senate Homeland Security and Governmental Affairs Committee. In the 112th Congress, S. 413 would make changes similar to those in S. 3480. H.R. 1136 would make many changes similar to those in H.R. 5136. The White House Proposal is broadly similar to the congressional proposals. However, it would not create a White House cybersecurity office and would transfer responsibilities to the DHS Secretary rather than to a new cybersecurity center within DHS. The Task Force Report recommends an increased focus on monitoring, support for DHS authority, and taking new and emerging technologies, such as cloud computing, into account. S. 1535 would require that agency information security programs assess the practices of contractors and third parties with respect to sensitive personally identifiable information as defined in the bill and ensure that any deficiencies are remediated.

Terrorism Risk Insurance Act of 2002


Major Relevant Provisions

- Provides federal cost-sharing subsidies for insured losses resulting from acts of terrorism.

(...continued)

Activities of the Executive Office of the President and the Department of Homeland Security (DHS)”). Weaknesses in FISMA implementation have been cited repeatedly by GAO in reports required by the act (see, for example, Government Accountability Office, Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements).

128 The bill included provisions from H.R. 4900, which was ordered reported by the House Oversight and Government Reform Committee.


Possible Updates

The act is intended to provide incentives for the development of insurance coverage for losses from acts of terrorism. Losses from cyber attacks are not specifically included, and some observers have raised concerns about whether some modification of the act would be appropriate.131

Cyber Security Research and Development Act, 2002

P.L. 107-305, 116 Stat. 2367, 15 U.S.C. §§278g,h], §7401 et seq.132

Major Relevant Provisions

- Requires the National Science Foundation (NSF) to award grants for basic research to enhance computer security and for improving undergraduate and master’s degree programs, doctoral research, and faculty development programs in computer and network security; and to establish multidisciplinary centers for research on computer and network security.

- Requires NIST to establish programs to award postdoctoral and senior research fellowships in cybersecurity and to assist institutions of higher learning that partner with for-profit entities to perform cybersecurity research; to perform intramural specified cybersecurity research; and to develop a checklist of security settings for federal computer hardware and software for voluntary use by federal agencies.

Possible Updates

A commonly expressed concern about federal research and development (R&D) relating to cybersecurity has been that it is insufficiently coordinated and prioritized, and focuses too little on understanding of fundamental principles and using them to develop transformational technologies. The George W. Bush Administration attempted to address the latter gap through the “leap-ahead” technology component of the Comprehensive Cybersecurity Initiative,133 The Obama Administration’s policy review134 also called for expanded, transformational research. Concerns have also been raised about the need to improve the process by which NIST creates checklists and other guidance and technical standards for federal IT systems.135

---

132 15 U.S.C. §§278g,h are part of the NIST Act (see p. 13).
134 The White House, Cyberspace Policy Review.
H.R. 4061 in the 111th Congress would have addressed those concerns by revising the act. A similar bill in the 112th Congress, H.R. 2096, would, as amended,

- expand NSF and NIST R&D programs in cybersecurity, including social and behavioral aspects of cybersecurity, identity management, testing and measurement, and control systems; and
- require NIST to develop automated security specifications for its cybersecurity standards, checklists, and associated data.

**E-Government Act of 2002**


**Major Relevant Provisions**

Serves as the primary legislative vehicle to guide federal IT management and initiatives to make information and services available online. Significant provisions include the following:

- Established the Office of Electronic Government within OMB, to be headed by an administrator with a range of IT management responsibilities, including cybersecurity.
- Established the interagency CIO (Chief Information Officer) Council and specified working with the National Institute of Standards and Technology (NIST) on security standards as one of its functions.
- Assigned agency CIOs responsibility for monitoring implementation of federal cybersecurity standards in their agencies.
- Contains various other requirements for security and protection of confidential information, including electronic authentication and privacy guidelines.
- Established a five-year personnel exchange program between federal agencies and private sector organizations to help agencies fill IT management training needs.
- Also included the “Federal Information Security Management Act of 2002 (FISMA).”

**Possible Update**

The *White House Proposal* would renew the personnel exchange program, which terminated at the end of 2007, and remove the current restriction in eligibility to management personnel. While this program would be applicable to any subdiscipline of IT, a widely held belief at present is that gaps in cybersecurity expertise are of particular concern. S. 1732 would revise the privacy provisions to account for the increased commercial availability of personally identifiable
information, which the bill defines broadly.\textsuperscript{136} It would also require agencies to designate chief privacy officers and create a council of them, and broaden OMB’s privacy responsibilities.

Identity Theft Penalty Enhancement Act

18 U.S.C. §§1028, 1028A.\textsuperscript{137}

Major Relevant Provisions

- Established penalties for \textit{aggravated} identity theft, in which a convicted perpetrator could receive additional penalties (two to five years’ imprisonment) for identity theft committed in relation to other federal crimes.\textsuperscript{138}

Possible Updates

While the number of reported incidents of identity theft fell in 2010, identity theft has generally been the fastest growing type of fraud in the United States over the past decade.\textsuperscript{139} FTC complaint data indicate that the most common fraud complaint received (19% of all consumer fraud complaints in 2010) has remained that of identity theft.\textsuperscript{140} In 2010, for instance, about 8.1 million Americans were reportedly victims of identity theft. This is a decrease of about 28% from the approximately 11.1 million who were victimized in 2009.\textsuperscript{141} Javelin Strategy and Research estimates that identity theft cost consumers about $37 billion in 2010.

The most recent congressional action taken to enhance the identity theft laws was through the Identity Theft Enforcement and Restitution Act of 2008 (Title II of P.L. 110-326). Among other elements, several of which were recommended by a presidential task force in 2007,\textsuperscript{142} the act authorized restitution to identity theft victims for their time spent recovering from the harm caused by the actual or intended identity theft. Legislation has not yet, however, adopted recommendations of the task force to

\textsuperscript{136} It would include “any information about an individual maintained by an agency.”
\textsuperscript{137} Prepared by Kristin M. Finklea, Analyst in Domestic Security (kfinklea@crs.loc.gov, 7-6259). For classification details, see 18 U.S.C. §1028 nt.
\textsuperscript{138} Examples of such federal crimes include theft of public property, theft by a bank officer or employee, theft from employee benefit plans, false statements regarding Social Security and Medicare benefits, several fraud and immigration offenses, and specified felony violations pertaining to terrorist acts.
\textsuperscript{139} For more information on identity theft, see CRS Report R40599, \textit{Identity Theft: Trends and Issues}, by Kristin M. Finklea.
Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions

• amend the identity theft and aggravated identity theft statutes so that thieves who misappropriate the identities of corporations and organizations—and not just the identities of individuals—can be prosecuted,\(^{143}\) and

• amend the aggravated identity theft statute by adding new crimes as predicate offenses\(^{144}\) for aggravated identity theft violations.\(^{145}\)

The task force recommended that Congress clarify the identity theft and aggravated identity theft statutes to cover both individuals and organizations targeted by identity thieves because the range of potential victims includes not only individuals but organizations as well. The task force cites “phishing” as a means by which identity thieves assume the identity of a corporation or organization in order to solicit personally identifiable information from individuals.\(^ {146}\)

In part because identity theft is a facilitating crime, and the criminal act of stealing someone’s identity often does not end there, investigating and prosecuting identity theft often involves investigating and prosecuting a number of related crimes. In light of this interconnectivity, the task force recommended expanding the list of predicate offenses for aggravated identity theft. The task force specifically suggested adding identity theft-related crimes such as mail theft,\(^ {147}\) counterfeit securities,\(^ {148}\) and tax fraud.\(^ {149}\)

The Task Force Report also recommends requiring restitution for victims of identity theft and computer fraud.\(^ {150}\) At present, the statute authorizes restitution but does not require it.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA)

42 U.S.C. §2000ee, 50 U.S.C. §403-1 et seq., §403-3 et seq., §404o et seq.\(^ {151}\)

Major Relevant Provisions

• Established the position of the Director of National Intelligence.

• Establishes mission responsibilities for some entities in the intelligence, homeland security, and national security communities.

• Discusses issues related to the collection, analysis, and sharing of security-related information.

\(^{143}\) This would involve revision of 18 U.S.C. §§1028 and 1028A.

\(^{144}\) A predicate offense can be described as a crime that is a component of a more serious offense. For example, in the case of money laundering, the crime that produces the funds that are to be laundered is the predicate offense.

\(^{145}\) This would involve revision of 18 U.S.C. §1028A.

\(^{146}\) The President’s Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, pp. 91 – 92.

\(^{147}\) 18 U.S.C. §1708.


\(^{149}\) 26 U.S.C. §7201, 7206-7207.


\(^{151}\) Prepared by John Rollins, Specialist in Terrorism and National Security (jrollins@crs.loc.gov, 7-5529). Classification of this act is complex. For details, see 50 U.S.C. §401 nt.
Establishes a Privacy and Civil Liberties Board within the Executive Office of the President.

Possible Updates

The act does not contain a single reference to cyber, cybersecurity, or related activities. Its stated purpose is to “reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes.” The act contains findings and recommendations offered in the 9/11 Commission Report152 and other assessments that address national and homeland security shortcomings associated with the terrorist attacks of September 11, 2001.

Numerous organizations, programs, and activities in the act currently address cybersecurity-related issues. IRPTA addresses many types of risks to the nation and threats emanating from man-made and naturally occurring events. The broad themes of the act could be categorized as how the federal government identifies, assesses, defeats, responds to, and recovers from current and emerging threats. The act might be updated to incorporate cybersecurity-related issues. However, any such update could affect numerous organizations and activities. 153

153 For more information on threats, responses, and issues associated with cyberterrorism, see CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John Rollins.
<table>
<thead>
<tr>
<th>Year</th>
<th>Popular Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/18/1878</td>
<td>Posse Comitatus Act (p. 10)</td>
</tr>
<tr>
<td>7/2/1890 and later</td>
<td>Antitrust Laws: (p. 11)</td>
</tr>
<tr>
<td></td>
<td>Sherman Antitrust Act, Wilson Tariff Act</td>
</tr>
<tr>
<td>3/3/1901</td>
<td>National Institute of Standards and Technology (NIST) Act (p. 13)</td>
</tr>
<tr>
<td>8/13/1912</td>
<td>Radio Act of 1912</td>
</tr>
<tr>
<td>2/23/1927</td>
<td>Radio Act of 1927</td>
</tr>
</tbody>
</table>

Table 2. Laws Identified as Having Relevant Cybersecurity Provisions

RS20590
R41886
RS20590

CRS-40
<table>
<thead>
<tr>
<th>Year</th>
<th>Popular Name</th>
<th>Law</th>
<th>Stat.</th>
<th>U.S.C.</th>
<th>Applicability and Notes</th>
<th>CRS Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/19/1934</td>
<td>Communications Act of 1934 (p.14)</td>
<td>Ch. 652</td>
<td>48 Stat. 1064</td>
<td>47 U.S.C. §151 et seq.</td>
<td>Established the Federal Communications Commission (FCC) and gave it regulatory authority over both domestic and international commercial wired and wireless communications. Provides the President with emergency powers over communications stations and devices. Governs protection by cable operators of information about subscribers.</td>
<td>RL32589, RL34693</td>
</tr>
<tr>
<td>1/27/1948</td>
<td>US Information and Educational Exchange Act of 1948 (p. 15)</td>
<td>Ch. 36</td>
<td>62 Stat. 6</td>
<td>22 U.S.C. §1431 et seq.</td>
<td>Restricts the State Department from disseminating public diplomacy information domestically and limits its authority to communicate with the American public in general. Has been interpreted by some to prohibit the military from conducting cyberspace information operations, some of which could be considered propaganda that could reach U.S. citizens, since the government does not restrict Internet access according to territorial boundaries.</td>
<td>R41674</td>
</tr>
<tr>
<td>9/8/1950</td>
<td>Defense Production Act of 1950</td>
<td>Ch. 932</td>
<td>64 Stat. 798</td>
<td>50 U.S.C. App. §2061 et seq.</td>
<td>Codifies a robust legal authority given the President to force industry to give priority to national security production and ensure the survival of security-critical domestic production capacities. It is also the statutory underpinning of governmental review of foreign investment in U.S. companies.</td>
<td>RS20587, RL31133</td>
</tr>
<tr>
<td>8/1/1956</td>
<td>State Department Basic Authorities Act of 1956 (p. 17)</td>
<td>P.L. 84-885</td>
<td>70 Stat. 890</td>
<td>22 U.S.C. §2651a</td>
<td>Specifies the organization of the Department of State, including the positions of coordinator for counterterrorism. As the Internet becomes increasingly international, concerns have been raised about the development and coordination of international efforts in cybersecurity by the United States.</td>
<td>R40989</td>
</tr>
<tr>
<td>Year</td>
<td>Popular Name</td>
<td>Law</td>
<td>Stat.</td>
<td>U.S.C.</td>
<td>Applicability and Notes</td>
<td>CRS Reports</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>7/4/1966</td>
<td>Freedom of Information Act (FOIA) (p. 17)</td>
<td>P.L. 89-487</td>
<td>80 Stat. 250</td>
<td>5 U.S.C. §552</td>
<td>Enables anyone to access agency records except those falling into nine categories of exemption, among them classified documents, those exempted by specific statutes, and trade secrets or other confidential commercial or financial information.</td>
<td>R41406</td>
</tr>
<tr>
<td>6/19/1968</td>
<td>Omnibus Crime Control and Safe Streets Act of 1968 (p. 19)</td>
<td>P.L. 90-351</td>
<td>82 Stat. 197</td>
<td>42 U.S.C. Chapter 46, §§3701 to 3797ee-1</td>
<td>Title I established federal grant programs and other forms of assistance to state and local law enforcement. Title III is a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both activities in general terms but that also permitted federal and state law enforcement officers to use them under strict limitations.</td>
<td>R41933</td>
</tr>
<tr>
<td>10/6/1972</td>
<td>Federal Advisory Committee Act (p. 20)</td>
<td>P.L. 92-463</td>
<td>86 Stat 770</td>
<td>5 U.S.C. App., §§1-16</td>
<td>Specifies conditions for establishing a federal advisory committee and its responsibilities and limitations. Requires open, public meetings and that records be available for public inspection. Has been criticized as potentially impeding the development of public/private partnerships in cybersecurity, particularly private-sector communications and input on policy.</td>
<td>R40520</td>
</tr>
<tr>
<td>Year</td>
<td>Popular Name</td>
<td>Law</td>
<td>Stat.</td>
<td>U.S.C.</td>
<td>Applicability and Notes</td>
<td>CRS Reports</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>12/31/1974</td>
<td>Privacy Act of 1974 (p. 20)</td>
<td>P.L. 93-579</td>
<td>88 Stat. 1896</td>
<td>5 U.S.C. §552a</td>
<td>Limits the disclosure of personally identifiable information (PII) held by federal agencies. Established a code of fair information practices for collection, management, and dissemination of records by agencies, including requirements for security and confidentiality of records.</td>
<td></td>
</tr>
<tr>
<td>10/21/1986</td>
<td>Electronic Communications Privacy Act of 1986 (ECPA) (p. 22)</td>
<td>P.L. 99-508</td>
<td>100 Stat. 1848</td>
<td>18 U.S.C. §§2510-2522, 2701-2712, 3121-3126</td>
<td>Attempts to strike a balance between privacy rights and the needs of law enforcement with respect to data shared or stored by electronic and telecommunications services. Unless otherwise provided, prohibits the interception of or access to stored oral or electronic communications, use or disclosure of information so obtained, or possession of electronic eavesdropping equipment.</td>
<td>R41733</td>
</tr>
</tbody>
</table>

*CRS-43*
<table>
<thead>
<tr>
<th>Year</th>
<th>Popular Name</th>
<th>Law</th>
<th>Stat.</th>
<th>U.S.C.</th>
<th>Applicability and Notes</th>
<th>CRS Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/8/1988</td>
<td>Computer Security Act of 1987</td>
<td>P.L. 100-235</td>
<td>101 Stat. 1724</td>
<td>15 U.S.C. §§272, 278g-3, 278g-4, 278h</td>
<td>Required NIST to develop and the Secretary of Commerce to promulgate security standards and guidelines for federal computer systems except national security systems. Also required agency planning and training in computer security (this provision was superseded by FISMA—see p. 32).</td>
<td></td>
</tr>
<tr>
<td>2/8/1996</td>
<td>Communications Decency Act of 1996 (p. 27)</td>
<td>P.L. 104-104 (Title V)</td>
<td>110 Stat. 133</td>
<td>See 47 U.S.C. §§223, 230</td>
<td>Intended to regulate indecency and obscenity on telecommunications systems, including the Internet. Has been interpreted to absolve Internet service providers and certain web-based services of responsibility for third-party content residing on those networks or websites.</td>
<td>R41499</td>
</tr>
<tr>
<td>Year</td>
<td>Popular Name</td>
<td>Law</td>
<td>Stat.</td>
<td>U.S.C.</td>
<td>Applicability and Notes</td>
<td>CRS Reports</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-------------</td>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>8/21/1996</td>
<td>Health Insurance Portability and Accountability Act of 1996 (HIPAA)</td>
<td>P.L. 104-191</td>
<td>110 Stat. 1936</td>
<td>42 U.S.C. §1320d et seq.</td>
<td>Required the Secretary of Health and Human Services to establish security standards and regulations for protecting the privacy of individually identifiable health information, and required covered health-care entities to protect the security of such information.</td>
<td>RL34120</td>
</tr>
<tr>
<td>Year</td>
<td>Popular Name</td>
<td>Law</td>
<td>Stat.</td>
<td>U.S.C.</td>
<td>Applicability and Notes</td>
<td>CRS Reports</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------</td>
<td>----------------</td>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>11/27/2002</td>
<td>Cyber Security Research and Development Act, 2002 (p. 34)</td>
<td>P.L. 107-305</td>
<td>116 Stat. 2367</td>
<td>15 U.S.C. §§278g, h, 7401 et seq.</td>
<td>Requires the National Science Foundation (NSF) to award grants for basic research and education to enhance computer security. Required NIST to establish cybersecurity research programs.</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Popular Name</td>
<td>Law</td>
<td>Stat.</td>
<td>U.S.C.</td>
<td>Applicability and Notes</td>
<td>CRS Reports</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Year</td>
<td>Popular Name</td>
<td>Law</td>
<td>Stat.</td>
<td>U.S.C.</td>
<td>Applicability and Notes</td>
<td>CRS Reports</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------</td>
<td>--------------------------</td>
<td>-----------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>


**Note:** Prepared by Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739) and Eric A. Fischer. Laws in *italics* are discussed in the text.

Author Contact Information

Eric A. Fischer
Senior Specialist in Science and Technology
efischer@crs.loc.gov, 7-7071

Acknowledgments

Contributing CRS staff include

- Patricia Moloney Figliola ("Communications Assistance for Law Enforcement Act of 1994"),
- Wendy R. Ginsberg ("Freedom of Information Act (FOIA),” “Clinger-Cohen Act (Information Technology Management Reform Act) of 1996"),
- John Rollins ("Department of Defense Appropriations Act, 1987,” “Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA)")
- Kathleen Ann Ruane ("Antitrust Laws and Section 5 of the Federal Trade Commission Act"),
- Gina Stevens ("Electronic Communications Privacy Act of 1986"),
- Rita Tehan (Table 2), and