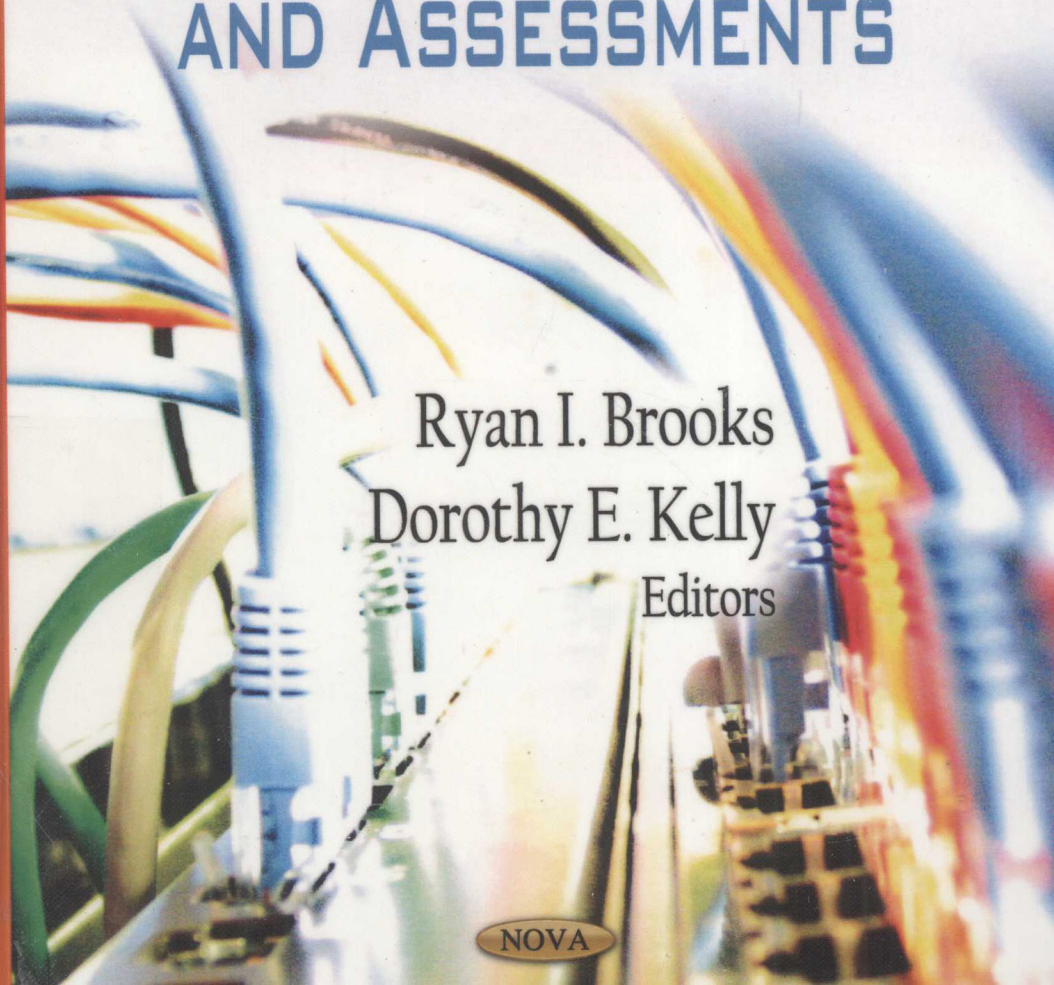
Defense, Security and Strategies

FEDERAL CYBERSECURITY

LEGAL CONSIDERATIONS AND ASSESSMENTS



Ryan I. Brooks
Dorothy E. Kelly
Editors

NOVA

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-62257-213-7

Published by Nova Science Publishers, Inc. † New York

DEFENSE, SECURITY AND STRATEGIES

FEDERAL CYBERSECURITY

LEGAL CONSIDERATIONS AND ASSESSMENTS

DEFENSE, SECURITY AND STRATEGIES

Additional books in this series can be found on Nova's website
under the Series tab.

Additional E-books in this series can be found on Nova's website
under the E-book tab.

AMERICAN POLITICAL, ECONOMIC, AND SECURITY ISSUES

Additional books in this series can be found on Nova's website
under the Series tab.

Additional E-books in this series can be found on Nova's website
under the E-book tab.

PREFACE

The federal government's role in protecting U.S. citizens and critical infrastructure from cyber attacks has been the subject of recent congressional interest. This book discusses selected legal issues that frequently arise in the context of recent legislation to address vulnerabilities of critical infrastructure to cyber threats, efforts to protect government networks from cyber threats, and proposals to facilitate and encourage sharing of cyber threat information amongst private sector and government entities.

Chapter 1- The federal government's role in protecting U.S. citizens and critical infrastructure from cyber attacks has been the subject of recent congressional interest. Critical infrastructure commonly refers to those entities that are so vital that their incapacitation or destruction would have a debilitating impact on national security, economic security, or the public health and safety. This report discusses selected legal issues that frequently arise in the context of recent legislation to address vulnerabilities of critical infrastructure to cyber threats, efforts to protect government networks from cyber threats, and proposals to facilitate and encourage sharing of cyber threat information amongst private sector and government entities. This report also discusses the degree to which federal law may preempt state law.

It has been argued that, in order to ensure the continuity of critical infrastructure and the larger economy, a regulatory framework for selected critical infrastructure should be created to require a minimum level of security from cyber threats. On the other hand, others have argued that such regulatory schemes would not improve cybersecurity while increasing the costs to businesses, expose businesses to additional liability if they fail to meet the imposed cybersecurity standards, and increase the risk that proprietary or confidential business information may be inappropriately disclosed.

Chapter 2- This Privacy Impact Assessment (PIA) examines the privacy implications of the United States Computer Emergency Readiness Team's (US-CERT's) EINSTEIN Program in accordance with Section 208 of the E-Government Act and the guidance for PIAs issued by the Office of Management and Budget (OMB). This PIA addresses for the EINSTEIN Program:

What and why the information is being collected;

The intended use of the agency information;

With whom the information will be shared;

What notice or opportunities for consent would be provided to individuals regarding information collected;

How that information is shared and secured; and

Whether a system of records is being created under section 552a of title 5, United States Code (the "*Privacy Act*").

Chapter 3- This is the Privacy Impact Assessment (PIA) for an updated version of the EINSTEIN System. EINSTEIN is a computer network intrusion detection system (IDS) used to help protect federal executive agency information technology (IT) enterprises. Pursuant to Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. § 3501, note), the Department of Homeland Security (DHS) must provide this publicly available PIA prior to initiating a new collection of information that uses information technology to collect, maintain or disseminate information that is in an identifiable form or collects identifiable information through the use of information technology. The original PIA for EINSTEIN 1, dated September 2004, explained that EINSTEIN 1 analyzes network flow information from participating federal executive government agencies and provides a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks.

The updated version, EINSTEIN 2, will incorporate network intrusion detection technology capable of alerting the United States Computer Emergency Readiness Team (US-CERT) to the presence of malicious or potentially harmful computer network activity in federal executive agencies' network traffic. EINSTEIN 2 principally relies on commercially available intrusion detection capabilities to increase the situational awareness of the US-CERT. This network intrusion detection technology uses a set of predefined signatures based upon known malicious network traffic. The signatures which will be implemented when EINSTEIN 2 goes "live" are based upon malicious computer code and are not based upon personally identifiable information (PII). Nor is the IDS programmed to specifically collect or locate PII. While

future signatures might be developed in response to threats that use what appears to be PII, the purpose of these signatures is to prevent malicious activity from reaching federal networks, not to collect or locate PII. For example, if the author of a computer security exploit chose to use PII in the delivery of malicious code, a signature may be developed in response to that exploit which could contain PII.1 Accordingly, while the IDS will collect some PII that is directly related to malicious code being transmitted to the federal networks, its main focus is to identify the malicious code and protect federal networks, not to collect PII. In identifying malicious code across the federal networks, EINSTEIN 2 increases situational awareness and provides an improved real-time ability to address computer network incidents on federal systems.

Chapter 4- Pursuant to Initiative Three of the Comprehensive National Cybersecurity Initiative, DHS is engaging in an exercise to demonstrate a suite of technologies that could be included in the next generation of the Department's EINSTEIN network security program. This demonstration, (commonly referred to as the —Initiative Three Exercise" or, more simply, as —the Exercise") will use a modified complement of system components currently providing the EINSTEIN 1 and EINSTEIN 2 capabilities, as well as a DHS test deployment of technology developed by the National Security Agency (NSA) that includes an intrusion prevention capability (collectively referred to as —the Exercise technology"). The purpose of the Exercise is to demonstrate the ability of an existing Internet Service Provider that is a designated as a Trusted Internet Connection Access Provider (TICAP) to select and redirect Internet traffic from a single participating government agency through the Exercise technology, for US-CERT to apply intrusion detection and prevention measures to that traffic and for US-CERT to generate automated alerts about selected cyber threats. This PIA is being conducted because the Exercise will analyze Internet traffic which may contain personally identifiable information (PII).

Chapter 5- The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) National Cyber Security Division (NCSD) launched the EINSTEIN program in 2004 as a computer network intrusion detection system to help protect federal executive agency information technology enterprises. NCSD deployed EINSTEIN in phases including EINSTEIN 1, EINSTEIN 2, and the Initiative 3 Exercise (Exercise), with each phase adding new functionality.

The first phase, EINSTEIN 1 was launched in 2004 and serves as an automated process for collecting computer network security information from

voluntarily participating federal executive agencies. EINSTEIN 1 collects network flow records,[1] which identify the source Internet Protocol (IP) address of the computer that connects to the federal system; the port the source uses to communicate; the time the communication occurred; the federal destination IP address; the protocol used to communicate; and, the destination port.

EINSTEIN 2, launched in 2008, incorporates network intrusion detection that monitors for malicious activity in network traffic to and from participating federal executive agencies. This gives the United States Computer Emergency Readiness Team (US-CERT) [2] the ability to analyze malicious activity occurring across the federal IT networks resulting in improved computer network security into the basic platform of the EINSTEIN program capabilities. This network intrusion detection technology uses a set of custom signatures[3] based upon known malicious network traffic. Each new level of EINSTEIN builds on the previous one but EINSTEIN 1 and 2 continue to operate as distinct programs as new capabilities are introduced to later versions.

In 2010, NCSD launched the Exercise to identify the ability of an existing Internet Service Provider to select and redirect internet traffic from a single participating government agency through the Exercise technology. The Exercise applied intrusion detection and prevention measures to that traffic and allowed for US-CERT to generate automated alerts about selected cyber threats. As the EINSTEIN program progresses EINSTEIN 1, 2 and eventually 3 will continue to work to prevent cyber threats from attacking the federal system and increase cybersecurity.

NCSD conducted Privacy Impact Assessments (PIAs) for each phase of the EINSTEIN program, which the DHS Privacy Office reviewed and approved. As NCSD looks ahead toward the next phase of the program to EINSTEIN [3], the DHS Privacy Office determined that conducting a Privacy Compliance Review (PCR) would be timely to ensure the accuracy of compliance documentation and transparency of the EINSTEIN program moving forward.[4]

The primary objective of the PCR was to assess NCSD's compliance with existing privacy compliance documentation, specifically the EINSTEIN 2 (May 19, 2008) and Initiative 3 Exercise (March 18, 2010) PIAs.[5] To address our objective, the DHS Privacy Office reviewed Standard Operating Procedures (SOPs), Concept of Operations for National Cybersecurity Protection System (NCPS) – which includes EINSTEIN capabilities, international agreements, and signature templates. The DHS Privacy Office also held a question and answer session with NPPD/NCSD leadership,

conducted two visits of the US-CERT analyst site, and interviewed US-CERT analysts who use, have access to, and are responsible for the accuracy of EINSTEIN program capabilities.

The review was conducted from May to July 2011 and was led by the DHS and NPPD Privacy Offices. Throughout the review, the DHS Privacy Office collaborated with the leadership of NPPD and NCSD including the: former US-CERT Director; Acting USCERT Director; US-CERT Deputy Chief of Operations; Network Security Deployment, System Sustainment and Operations Section Chief; and Director, Network Security Deployment. NPPD/NCSD recently hired a senior privacy analyst to work on privacy protections and issues for the EINSTEIN program. This review occurred before the analyst could be fully integrated into the general practices of NCSD.

Chapter 6- An intrusion-detection system known as EINSTEIN 2.0 used to protect civilian unclassified networks in the Executive Branch against malicious network activity complies with the Fourth Amendment to the Constitution, the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of chapter 206 of title 18, United States Code, provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system.

CONTENTS

In: Federal Cybersecurity
Editors: R. I. Brooks and D. E. Kelly
ISBN: 978-1-62257-213-7

Chapter 1

CYBERSECURITY: SELECTED LEGAL ISSUES*

Edward C. Liu, Gina Stevens, Kathleen Ann Ruane, Alissa M. Dolan and Richard M. Thompson II

SUMMARY

The federal government's role in protecting U.S. citizens and critical infrastructure from cyber attacks has been the subject of recent congressional interest. Critical infrastructure commonly refers to those entities that are so vital that their incapacitation or destruction would have a debilitating impact on national security, economic security, or the public health and safety. This report discusses selected legal issues that frequently arise in the context of recent legislation to address vulnerabilities of critical infrastructure to cyber threats, efforts to protect government networks from cyber threats, and proposals to facilitate and encourage sharing of cyber threat information amongst private sector and government entities. This report also discusses the degree to which federal law may preempt state law.

It has been argued that, in order to ensure the continuity of critical infrastructure and the larger economy, a regulatory framework for selected critical infrastructure should be created to require a minimum level of security from cyber threats. On the other hand, others have

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, CRS Report for Congress R42409, prepared for Members and Committees of Congress, from www.crs.gov, dated March 14, 2012.

argued that such regulatory schemes would not improve cybersecurity while increasing the costs to businesses, expose businesses to additional liability if they fail to meet the imposed cybersecurity standards, and increase the risk that proprietary or confidential business information may be inappropriately disclosed.

In order to protect federal information networks, the Department of Homeland Security (DHS), in conjunction with the National Security Agency (NSA), uses a network intrusion system that monitors all federal agency networks for potential attacks. Known as EINSTEIN, this system raises significant privacy implications—a concern acknowledged by DHS, interest groups, academia, and the general public. DHS has developed a set of procedures to address these concerns such as minimization of information collection, training and accountability requirements, and retention rules. Notwithstanding these steps, there are concerns that the program may implicate privacy interests protected under the Fourth Amendment.

Although many have argued that there is a need for federal and state governments, and owners and operators of the nation's critical infrastructures, to share information on cyber vulnerabilities and threats, obstacles to information sharing may exist in current laws protecting electronic communications or in antitrust law. Private entities that share information may also be concerned that sharing or receiving such information may lead to increased civil liability, or that shared information may contain proprietary or confidential business information that may be used by competitors or government regulators for unauthorized purposes.

Several bills in the 112th Congress would seek to improve the nation's cybersecurity, and may raise some or all of the legal issues mentioned above. For example, H.R. 3523 (Rogers (Mich.)) addresses information sharing between the intelligence community and the private sector. H.R. 3674 (Lungren) includes provisions regarding the protection of critical infrastructure, as well as information sharing. S. 2102 (Feinstein) seeks to facilitate information sharing. S. 2105 (Lieberman) includes the information sharing provisions of S. 2102, as well as provisions relating to the protection of critical infrastructure and federal government networks. S. 2151 (McCain) also addresses information sharing among the private sector and between the private sector and the government. Many of these bills also include provisions specifically addressing the preemption of state laws.

INTRODUCTION

For many, the Internet has become inextricably intertwined with daily life. Many rely on it to perform their jobs, pay their bills, send messages to loved ones, track their medical care, and voice political opinions, among a host of other activities. Likewise, government and business use the Internet to maintain defense systems, protect power plants and water supplies, and keep other types of critical infrastructure running.[1] Consequently, the federal government's role in protecting U.S. citizens and critical infrastructure from cyber attacks has been the subject of recent congressional interest.[2]

This report discusses selected legal issues that frequently arise in the context of legislation to address vulnerabilities of private critical infrastructure to cyber threats, efforts to protect government networks from cyber threats, and proposals to facilitate and encourage sharing of cyber threat information amongst private sector and government entities. This report also provides an overview of the ways in which federal laws of these types may preempt or affect the applicability of state law.

LEGAL ISSUES RELATED TO PROTECTING CRITICAL INFRASTRUCTURE

Although no federal statute currently imposes a generally applicable obligation on businesses in the private sector to take measures to protect themselves from cyber vulnerabilities, Congress has chosen to impose regulatory standards regarding the security, including the cybersecurity, of specific sectors or types of private entities.[3] For example,[4] chemical facilities are subject to chemical facility anti-terrorism standards (CFATS) promulgated by the Department of Homeland Security (DHS), which include provisions requiring chemical facilities to take measures to protect against cyber threats.[5] Electrical utilities are required to comply with reliability standards, including standards to protect against cyber incidents, set by the North American Electrical Reliability Corporation (NERC).[6] Similarly, the Maritime Transportation Security Act (MTSA) gives the Coast Guard the authority to regulate the security of maritime facilities and vessels, including requiring security plans that contain provisions for the security of communications systems used in those facilities.[7]

Proposals that focus on the increased cybersecurity of certain sectors of the economy are frequently justified on the grounds that those private entities, including energy, transportation, or communication providers, comprise the nation's critical infrastructure. If the incapacity or destruction of such systems or assets would have a debilitating impact on national security, economic security, or public health and safety, it would be in the national interest to ensure that such critical infrastructure was adequately protected. Consequently, it has been argued that a regulatory framework governing selected critical infrastructure entities is needed to ensure that these private entities take measures adequate to maintain a minimum level of security from cyber threats, in order to protect the rest of the economy.[8]

On the other hand, others have argued that such regulatory schemes would not improve cybersecurity and would also increase the costs of doing business for these sectors of the economy.[9]

There are also concerns that businesses would face additional exposure to civil liability from private suits if they failed to meet the imposed standards. As many of these regulatory schemes provide regulatory agencies with access to information held by the regulated entities, concerns have also been raised about the inappropriate disclosure of proprietary or confidential business information.

The concerns raised by these issues have shaped the existing legal schemes regulating the security of specific categories of critical infrastructure, and have also informed recent legislative proposals to address widely reported weaknesses in the security of critical infrastructure from cyber threats. A brief overview of each of these issues is provided in the next sections of this report. The report will then examine how recent cybersecurity legislation would specifically address some or all of these issues.

Deference to Agency Decisions

Several of the bills that would establish a regulatory scheme for the cybersecurity of critical infrastructure provide the agencies charged with administering the program with the discretion to identify those private entities that would fall within the scope of a particular bill and that will, therefore, be subject to the requirements that would be imposed under the bill. Being subject to the regulations may have significant cost, liability, or other implications for the private entity that has been designated as covered critical infrastructure; such entities may seek to challenge their designation as covered

critical infrastructure through redress mechanisms created in the statute or through judicial review of agency action under the Administrative Procedure Act (APA).[10] Entities may also seek judicial review of agency actions in the context of enforcement actions taken against them under the various regulatory schemes.

Depending upon the legislative language delegating regulatory authority to the agency, a court will evaluate an agency's decision under varying standards of review. In the context of regulating the security of critical infrastructure, a more deferential standard of review of agency determinations typically means that regulated private entities would have less recourse in the event that they wanted to challenge an agency's determination. On the other hand, a less deferential standard of review may extend the time to implement particular security standards if the agency encounters delays caused by litigation. Examples of the different types of judicial review that may be involved are discussed below.

Availability of Judicial Review[11]

As a general matter, there is a "'strong presumption that Congress intends judicial review' of administrative action."[12] This presumption is embodied in the Administrative Procedure Act (APA), which provides that "final agency action for which there is no other adequate remedy in a court [is] subject to judicial review."[13] The APA provides two exceptions to the presumption of availability of judicial review of agency action: (1) "to the extent that ... statutes preclude judicial review" and (2) "where agency action is committed to agency discretion by law."[14] However, judicial review of an unreviewable determination may occur if there is a constitutional issue.[15]

Under the APA, judicial review of agency actions may be unavailable if such review is specifically precluded by statute.[16] This exemption requires the existence of an explicit statutory provision prohibiting judicial review of agency action. Additionally, even where judicial review has not been explicitly barred, the APA precludes judicial review where the decision has been committed to agency discretion by law.[17] This second exemption has been interpreted by the Supreme Court to be a very narrow exception, and applies only in situations where the statute provides no law for a reviewing court to apply.18 For example, in Webster v. Doe,19 the Supreme Court held that firing decisions made by the Director of Central Intelligence were unreviewable because the National Security Act provided that the Director "may, in his discretion, terminate the employment of any officer or employee of the [Central Intelligence Agency] whenever he shall deem such termination

necessary or advisable in the interests of the United States."20 The Court held that such a statute "exuded deference" and noted:

> Short of permitting cross-examination of the Director concerning his views of the Nation's security and whether the discharged employee was inimical to those interests, we see no basis on which a reviewing court could properly assess an Agency termination decision.[21]

Since the statute contained no standards a court could apply to evaluate the Director's decision, the Court determined that these decisions had been committed to agency discretion by law, and were consequently unreviewable.

Questions of Fact

Where a statute does provide judicially administrable standards, agency determinations of factual questions are typically reviewed under the "substantial evidence" or "abuse of discretion standards."[22] In the administrative context, substantial evidence review and abuse of discretion review occur in factually distinct circumstances. Substantial evidence is required when an agency engages in either formal rulemaking or an adjudicatory hearing.[23] In contrast, abuse of discretion applies in cases of informal rulemaking and decisions.[24]

Some courts appear to consider substantial evidence a more demanding standard than abuse of discretion, but the consistent theme of both standards is that the court is not free to substitute its judgment in place of the agency's.[25] In terms of analysis, the substantial evidence and abuse of discretion standards are both less stringent than *de novo* review, which would allow a court to look at the evidence anew and come to its own conclusions. Nevertheless, the Supreme Court has described these standards as requiring "more than a mere scintilla" of support and comparable to the standard a trial judge must meet to sustain a jury's verdict.[26] In the federal courts, a jury verdict will not be disturbed if "reasonable and fair-minded persons in exercise of impartial judgment" might have come to the same conclusion as the jury.[27]

Interpretations of Law

Agencies may also exercise discretion in interpreting the terms used in a statute. In the context of the proposals to regulate the cybersecurity of critical infrastructure, which are discussed in more detail below, there are a number of provisions that may require the Secretary of Homeland Security (the Secretary) to use her discretion to interpret the language of the bills. For