AN A.S. PRATT PUBLICATION
OCTOBER 2015
VOL. 1 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 | NUMBER 2 | OCTOBER 2015

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Aaron P. Simpson and Adam H. Solomon, *Dealmakers Ignore Cyber Risks at Their Own Peril*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [46] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Cybersecurity and Government "Help" – Engaging with DOJ, DHS, FBI, Secret Service, and Regulators – Part I

By Alan Charles Raul and Tasha D. Manoranjan*

In this two-part article, the authors provide an overview of government cybersecurity resources and encourage companies to consider whether and when it makes sense to take advantage of this assistance. This first part of the article discusses the jurisdictional landscape and cybersecurity resources available from the Department of Justice and the Department of Homeland Security. The second part, which will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report*, will discuss cybersecurity resources available from the Federal Bureau of Investigation, the United States Secret Service, and regulators.*

Rampant cybersecurity incidents have not only ensnared a growing number of private companies and public sector organizations, but they have also given rise to an expanding slate of government agencies with roles to investigate, monitor and "help" companies defend themselves against and respond to serious breaches. Given President Obama's statement that "America's economic prosperity in the 21st century will depend on cybersecurity," it is fair and reasonable that the private sector companies should be able to expect substantial assistance from the government in defending themselves against cyber-attacks.[1] Nonetheless, "Help" is in quotes here because inviting government attention – even of the friendly variety – is often fraught with concern over potential two-edged consequences.

---

* Alan Charles Raul, a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, is a partner at Sidley Austin LLP, where he is the leader of the Privacy, Data Security and Information Law practice. Tasha D. Manoranjan is an associate in the firm's Privacy, Data Security and Information Law practice. Resident in the firm's Washington, D.C., office, the authors may be reached at araul@sidley.com and tmanoranjan@sidley.com, respectively.

[1] Alan Charles Raul, *Cyberdefense Is a Government Responsibility*, Wall St. J. (Jan. 5, 2015), *available at* http://www.wsj.com/articles/alan-charles-raul-cyberdefense-is-a-government-responsibility-1420502942 ("Regulatory agencies including the Federal Trade Commission, the Securities and Exchange Commission and state attorneys general think that investigating the corporate victims of cyberattacks for putative violations of consumer and investor protection laws is the best way to shore up the economy's cyberdefenses. There is little evidence this approach is effective.").

In general, however, law enforcement agencies do not turn on the victims of cybercrimes,[2] but the approach, perspective and responsibilities of regulatory agencies can be more complex.[3] As noted below, however, some government officials have suggested that companies that cooperate with law enforcement may receive favorable consideration from their regulators. This governmental recommendation should obviously be considered carefully, on a case-by-case basis, depending on the relevant circumstances and a company's legal obligations and best interests.

THE JURISDICTIONAL LANDSCAPE

In any event, the jurisdictional landscape surrounding cybersecurity is ever-evolving, and companies seeking to comply with cybersecurity requirements may feel overwhelmed by the spectre of the Department of Justice ("DOJ"), Department of Homeland Security ("DHS"), Federal Bureau of Investigation ("FBI"), the Secret Service, and various federal agencies (such as the Securities and Exchange Commission and FINRA) monitoring compliance with a myriad of laws, regulations, and guidance. However, there are a variety of government resources available to the savvy company that seeks to avail itself of such opportunities. Indeed, the government welcomes public-private partnerships in cybersecurity efforts; President Obama said at a February 2015 White House cybersecurity summit involving government, companies and consumer groups that such partnerships are essential: "There's only one way to defend America from these cyber threats, and that is through government and industry

---

[2] Jimmy Hoover, *FBI Won't Treat Data Breach Victims As Targets, Official Says*, Law360 (May 27, 2015) (noting that FBI Cybersecurity Division Deputy Assistant Director Donald Good said the FBI has begun treating companies that suffer a data breach like traditional crime victims rather than negligent data custodians.); Robert S. Mueller, Dir., Fed. Bureau of Investigation, RSA Cyber Security Conference: Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies (Mar. 1, 2012) ("We do not want you to feel victimized a second time by an investigation. We will minimize the disruption to your business, and we will safeguard your privacy. Where necessary, we will seek protective orders to preserve trade secrets and business confidentiality."); Matthew Noyes & Ari Baranoff (United States Secret Service), *Corporate-Government Engagement/Public-Private Partnerships*, *in Cybersecurity: A Practical Guide to the Law of Cyber Risk* 4-1, 4-6 (Ed McNicholas & Vivek Mohan eds., 2015) ("Whether or not a particular case merits federal criminal investigation into the perpetrator, the first priority of the Secret Service is to protect the victim and mitigate losses. . . Recognizing the potential reputational harms that companies face, the Secret Service takes the privacy and confidentiality of victim companies seriously".).

[3] Mary Ellen Callahan, former Chief Privacy Officer at DHS noted, "On one hand [the government is] reaching out as a friend and collaborator to work with companies. . .On the other hand, the same government has an enforcement arm outstretched with the FTC, the SEC[,] that if you do not comply, there can be repercussions, possible lawsuits and other regulatory action taken against you." Tyler Pager, *Private sector remains wary of government efforts to increase cybersecurity collaboration*, Medill National Security Zone (March 19, 2015), http://nationalsecurityzone.org/site/private-sector-remains-wary-of-government-efforts-to-increase-cybersecurity-collaboration/.

working together, sharing appropriate information as true partners."[4] This article provides an overview of such government resources, and encourages companies to consider whether and when it makes sense to take advantage of this assistance.

It should also be noted that even the half dozen or so federal agencies highlighted here are only just some of the agencies relevant to cybersecurity coordination and cooperation with the private sector. Owners and operators in certain critical infrastructure sectors (and/or their trade associations) will often have direct and particularly close working relationships with their "sector-specific agencies."[5] For example, the Securities Industry and Financial Markets Association ("SIFMA"), speaks of the need to "establish a robust partnership between the industry and government . . . to mitigate cyber threats: the industry will not be fully effective without the government's help, and vice versa."[6] The scope of this article, however, will focus on the resources and considerations applicable to individual companies that experience cyber incidents, or recognize the need to plan ahead for that inevitable contingency, rather than on public-private cybersecurity information sharing, or on the special government relationships for critical infrastructure.

DEPARTMENT OF JUSTICE

The Department of Justice's Cybersecurity Unit published guidance in April 2015 titled "Best Practices for Victim Response and Reporting of Cyber Incidents," which serves as a resource for companies seeking assistance and collaboration with the department.[7] The DOJ recommends having well-established, actionable plans and procedures for managing and responding to a cyber intrusion, which can help "limit damage to their computer networks, minimize work stoppages, and maximize the ability of law enforcement to locate and apprehend perpetrators."[8] Companies can

---

[4] Dian Schaffhauser, *Stanford-Hosted Cybersecurity Summit Calls for Government-Private Sector Teamwork*, Campus Technology (February 17, 2015), http://campustechnology.com/articles/2015/02/17/stanford-hosted-cybersecurity-summit-calls-for-government-private-sector-teamwork.aspx.

[5] *See, inter alia*, Exec. Order No. 13, 636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 33 (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf; Securities Industry and Financial Markets Association; Financial Services – Information Sharing and Analysis Center; Financial Industry Regulatory Authority; Federal Energy Regulatory Commission.

[6] *See* Kenneth E. Bentsen, Jr., President & CEO, SIFMA, *Statement Before the Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit of the U.S. House of Representatives*, 2 (May 19, 2015), *available at* http://financialservices.house.gov/uploadedfiles/hhrg-114-ba15-wstate-kbentsen-20150519.pdf.

[7] Cybersecurity Unit, Computer Crime & Intellectual Prop. Section, Criminal Div., Dep't of Justice, Best Practices for Victim Response and Reporting of Cyber Incidents (2015), *available at* http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf.

[8] *Id.* at 1.

consult this guidance for helpful tips and a checklist in establishing and maintaining an incident response plan. Additionally, the DOJ's Computer Crime and Intellectual Property Section works with companies to investigate and prosecute cybercrime.

The DOJ encourages organizations to establish a relationship with local federal law enforcement offices before they suffer a cyber incident; "[h]aving a point-of-contact and a pre-existing relationship with law enforcement will facilitate any subsequent interaction that may occur if an organization needs to enlist law enforcement's assistance."[9] In this regard, the DOJ encourages organizations to take advantage of regular outreach by the Federal Bureau of Investigation's Infragard chapters and Cyber Task Forces in each of the FBI's 56 field offices, as well as the Secret Service's Electronic Crimes Task Forces. Relationships with law enforcement agencies assist in establishing and maintaining information-sharing, which benefits potential and actual victim organizations.

If a company is the victim of a cyber breach, the DOJ recommends contacting law enforcement immediately. This can benefit the victim organization: "Law enforcement may be able to use legal authorities and tools that are unavailable to non-governmental entities and to enlist the assistance of international law enforcement partners to locate stolen data or identify the perpetrator."[10] The DOJ also notes as a benefit to companies that cooperation with law enforcement "may be viewed more favorably by regulators looking into a data breach."[11] Additionally, the DOJ points to 47 state data breach notification laws that require companies to notify customers whose data is compromised by an intrusion, and notes that many data breach laws allow notification to be delayed if law enforcement concludes that such notice would impede an ongoing investigation. Companies should consult with counsel to determine their responsibilities under state data breach notification laws.

DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security's National Cybersecurity & Communications Integration Center ("NCCIC") serves as a 24/7 operation for cybersecurity information sharing, incident response, and incident coordination. The NCCIC "shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions."[12] Victim organizations can share and receive information about an ongoing incident with NCCIC, and receive help such as technical assistance to mitigate the effects of cyber crime. NCCIC "sits at

[9] *Id.* at 5.
[10] *Id.* at 11.
[11] *Id.*
[12] Department of Homeland Security, "Information Sharing," *available at* http://www.dhs.gov/topic/-cybersecurity-information-sharing (last accessed July 6, 2015).

the intersection of cyber communities, with representatives from the private sector and other government entities physically present on the NCCIC floor and connected virtually."[13] In 2014, NCCIC received over 97,000 incident reports and issued around 12,000 actionable cyber-alerts.[14] In January 2015, President Obama proposed cybersecurity legislation to provide protections for private entities against civil or criminal liability for voluntary sharing of cybersecurity information with NCCIC. Such legislation has not been passed yet.

One part of NCCIC is the United States Computer Emergency Readiness Team ("US-CERT"), which coordinates cyber information sharing and proactively addresses cyber threats. Companies can report a data breach to DHS through the US-CERT Web site or by phone.[15] DHS may then let the company know if related activity has been seen elsewhere, and share relevant information. If a company requests assistance in managing a particularly significant incident, DHS can send a team onsite. Companies can share information with DHS under the Protected Critical Infrastructure Information ("PCII") Program, which supports voluntary information-sharing between infrastructure owners and operators, and the government. The PCII Program facilitates DHS's ability to work with infrastructure owners and operators to identify vulnerabilities, mitigation options and protections. However, regardless of whether information is submitted through the PCII Program or separately, DHS does not send risk alerts with company names.[16]

US-CERT also manages the Critical Infrastructure Cyber Community ("C^3") Voluntary Program to enhance critical infrastructure cybersecurity and support the adoption of the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework ("the Framework"). The C^3 Voluntary Program was established as part of an executive order signed by President Obama in 2013, establishing enhanced cybersecurity support for critical infrastructure industries.[17] The C^3 Voluntary Program helps organizations that want to use the Framework by connecting them to cyber risk management capabilities with DHS and other government and private

---

[13] Written testimony of NPPD Under Secretary Suzanne Spaulding and NPPD Deputy Under Secretary for Cybersecurity & Communications Phyllis Schneck for a House Committee on Homeland Security hearing titled "*Examining the President's Cybersecurity Information Sharing Proposal*" (February 25, 2015), http://www.dhs.gov/news/2015/02/25/written-testimony-nppd-under-secretary-and-deputy-under-secretary-cybersecurity.

[14] *Id.*

[15] United States Computer Emergency Readiness Team Web site: www.us-cert.gov; Phone: (888) 282-0870.

[16] The authors thank DHS for information graciously provided by the Office of Cybersecurity and Communications.

[17] Exec. Order No. 13, 636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 33 (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

entities. The C[3] Voluntary Program's primary focus is critical infrastructure, but later phases of the Program aim to reach businesses of all sizes interested in using the Framework.[18] Through the C[3] Voluntary Program, DHS's National Protection and Programs Directorate ("NPPD") offers critical infrastructure industries risk assessments and assistance.[19] These assessments "provide critical infrastructure owners and operators with invaluable information about their cybersecurity posture in relation to the Framework, and they offer concrete areas for improvement."[20]

On February 12, 2015, President Obama signed an executive order entitled, "Promoting Private Sector Cybersecurity Information Sharing," which directed the Secretary of Homeland Security to "strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs)."[21] The creation of ISAOs was sparked by DHS's success with Information Sharing and Analysis Centers ("ISACs"), in which critical infrastructure owners and operators joined with DHS to share information about cyber threats. ISAOs will be more inclusive, such that organizations from all non-profit and for-profit sectors can participate and benefit.[22] DHS will select an organization to serve as the ISAO Standards Organization, which will identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs.[23] Companies that participate in these information-sharing programs with DHS can utilize lessons learned to reduce their cyber risk, but should recognize that DHS's efforts and attention are generally focused on mitigating national-level risk associated with high-consequence threats.[24]

On February 25, 2015, President Obama directed the Director of National Intelligence ("DNI") to establish the Cyber Threat Intelligence Integration Center ("CTIIC"). CTIIC will provide "integrated all-source intelligence analysis" regarding

---

[18] *Critical Infrastructure Cyber Community Voluntary Program*, U.S. Computer Emergency Readiness Team, https://www.us-cert.gov/ccubedvp.

[19] Written testimony of NPPD Office of Cybersecurity & Communications Assistant Secretary Andy Ozment for a Senate Committee on Appropriations, Subcommittee on Homeland Security hearing titled "*From Protection to Partnership: Funding the DHS role in Cybersecurity*" (April 15, 2015), http://www.dhs.gov/news/2015/04/15/written-testimony-nppd-senate-appropriations-subcommittee-homeland-security-hearing.

[20] *Id.*

[21] Exec. Order No. 13,691, Promoting Private Sector Cybersecurity Information Sharing, 80 Fed. Reg. 9349 (Feb. 13, 2015), *available at* http://fas.org/irp/offdocs/eo/eo-13691.htm.

[22] Department of Homeland Security, "Information Sharing and Analysis Organizations," *available at* http://www.dhs.gov/isao (last accessed July 6, 2015).

[23] *Id.*

[24] Matthew Noyes & Ari Baranoff (United States Secret Service), *Corporate-Government Engagement/-Public-Private Partnerships*, *in Cybersecurity: A Practical Guide to the Law of Cyber Risk* 4-1, 4-7 (Ed McNicholas & Vivek Mohan eds., 2015).

cyber threats, and will work with NCCIC and other cyber-focused government task forces to protect U.S. citizens and companies from cyber attacks.[25] CTIIC will support NCCIC and provide it and other government entities with cybersecurity intelligence; it will not directly engage U.S. private sector companies to obtain or provide information.[26]

DHS provides information with the private sector to detect and counter cyber attacks. DHS "provides information to commercial cybersecurity companies so they can better protect their customers through the Enhanced Cybersecurity Services program, or ECS; and maintains a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends."[27] Through ECS, DHS shares sensitive and classified government cyber threat indicators of malicious activity with several commercial service providers, who can then implement appropriate countermeasures.[28] Private companies across the 16 critical infrastructure sectors can take advantage of this program by contacting the program office via email.[29] DHS prides itself on the trust placed in it by the private sector, derived "in large part from [DHS's] emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information."[30]

* * *

The second part of this article, which will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*, will discuss the cybersecurity resources available from the Federal Bureau of Investigation, the United States Secret Service, and regulators.

---

[25] Press Release, Office of the Press Secretary, The White House, FACT SHEET: Cyber Threat Intelligence Integration Center (February 25, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

[26] *Id.*

[27] Written testimony of NPPD Under Secretary Suzanne Spaulding and NPPD Deputy Under Secretary for Cybersecurity & Communications Phyllis Schneck for a House Committee on Homeland Security hearing titled "*Examining the President's Cybersecurity Information Sharing Proposal*" (February 25, 2015), http://www.dhs.gov/news/2015/02/25/written-testimony-nppd-under-secretary-and-deputy-under-secretary-cybersecurity.

[28] The Department of Homeland Security is reportedly reorganizing the Office of Cybersecurity and Communications, the office responsible for government-wide cybersecurity. Under the reported reorganization, ECS and the Critical Infrastructure Cyber Community Voluntary Program would be merged into the National Protection and Programs Directorate. NCCIC would remain within the Office of Cybersecurity and Communications.

[29] ECS_Program@hq.dhs.gov.

[30] *See supra* note 27.