Bloomberg BNA

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 15 PVLR 1886, 9/26/16. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Coal Plant Cybersecurity

The obligation to protect electronically stored data is one thing that doesn't change after a coal plant is shut down. In order to understand the legal rules that apply it's helpful to divide the sources of electronically stored information available in plants into three categories: the operational sources, the personal information sources and the business information sources, the authors write.

Cybersecurity

Cybersecurity, Electronic Data and the Closure of Coal Plants

BY JOEL DEJESUS AND J. WYLIE DONALD

The breakers have been thrown. The turbines have spun down. The steam traps are quiet. Your coal plant is shut down. A lot of things will be different. One thing that has not changed, however, is the obligation to protect electronically stored data. ''In a plant in the middle of demolition?'' you ask. ''Yes.'' Let us explain.

Joel deJesus is a partner at Dinsmore & Shohl LLP and a former director of compliance enforcement at the North American Electric Reliability Corporation.

J. Wylie Donald is a partner at McCarter & English LLP and leads the firm's Coal Plant Demolition and Redevelopment team.

Risks and Disposal

The National Institute of Science and Technology (NIST) in its 2014 Guidelines for Media Sanitation (Guidelines) describes the improper disposal of electronic media as a ''rich source'' of intelligence.

An often rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media, or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information. R. Kissel, et al., NIST, *Guidelines for Media Sanitization* at 5, NIST Special Publication 800-88, Rev. 1 (Dec. 2014).

It is not hard to find confirmation of NIST's viewpoint. Computer forensics firm Kessler International bought 100 hard drives on eBay. Lucas Mearian, *Survey: 40% of hard drives bought on eBay hold personal, corporate data*, ComputerWorld (Feb. 9, 2009). Forensic techniques recovered sensitive data on some devices. On other computers, however, personal information and corporate spreadsheets were recovered just by booting up the hard drive. *Id.*

Utilities are not immune to such problems. An early debacle involved the sale of 230 hard drives to a salvor, which in turn sold 84 of them on eBay. Bradley Mitchell, *Idaho utility hard drives—and data—turn up on eBay*, Computerworld (May 4, 2006). One of the purchasers, a university information technology director, found on the drives grid diagrams, confidential law department data and employee information including Social Security numbers. *Id.*

COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423

Since the approval of the North American Electric Reliability Corporation (NERC) Reliability Standards in 2007, things have gotten much better. But they are still not perfect. For example, in 2012 a utility settled a critical infrastructure protection (CIP) violation for $65,000 where it, among other things, failed to delete sensitive data from a hard drive, which it had returned to the vendor. NERC Violation ID WECC201002817, Notice of Penalty, FERC Docket No. NP12-47-000, (Sept. 28, 2012). As recently as this past February, NERC found that a vendor had left a responsible entity's premises with a failed Critical Asset storage switch, which had not been erased. NERC Violation ID RFC2015014617, Find Fix, Track and Report (Feb. 29, 2016).

In order to understand the legal rules that apply it is helpful to divide the sources of electronically stored information available in plants into three categories: the operational sources, the personal information sources and the business information sources. Plants come in all shapes and sizes. Small electric utilities may operate out of a single facility with employee and customer information in the same building as the generating plant. Large utilities with multiple facilities and sites may keep only operational information at the plant and all other business and employee information at an entirely separate facility, and some regulatory requirements may require that certain other business information not be kept at generator plant sites.

To understand the legal rules that apply it is helpful to divide the sources of electronically stored information available in plants into three categories: the operational sources, the personal information sources and the business information sources.

The NIST Guidelines for Media Sanitation break down the various equipment found in an enterprise and provide specific guidance on how to sanitize each type. Among other things, the enterprise must address networking devices (routers and switches), mobile devices (phones and tablets), office equipment (copiers, fax machines, phones), and all types of storage (magnetic, optical, solid state, RAM and ROM). Guidelines, Appendix A. Sanitizing is defined in the Guidelines as rendering access to data ''infeasible'' ''for a given level of effort.'' Guidelines, Appendix B at 44. In lay terms, hard drives, for example, are demagnetized, or even less technically, hard drives are ''wiped.''

Operational Information

A generation owner seeking to decommission a generating plant should be mindful of its obligations under the Reliability Standards promulgated by NERC. We focus in this article on what Reliability Standards requirements come into play when the generation owner decides to close down the plant and what it takes for the generation owner to discontinue its compliance responsibility relative to the plant.

Continued Compliance

A common misconception is that a generation owner's compliance responsibility somehow expires when the plant is decommissioned. In fact, a number of Reliability Standard requirements related to cybersecurity are actually triggered by a decommissioning. Accordingly, the generation owner should take stock of its compliance obligations whenever it contemplates a plant closure.

Reliability Standard CIP-010-2 governs configuration change management and vulnerability assessments for key industrial control systems used to operate bulk electric system (BES) components (like generators). This Standard requires responsible entities to prepare and maintain baseline configurations and to implement formal procedures for authorizing and documenting changes to these baseline configurations. The decommissioning of the electronically stored data within a plant would likely trigger this change management process. A key component of this change management process would be to ensure that any cybersecurity controls would not be adversely affected by the configuration change.

In addition, Reliability Standard CIP-011-2 provides for protection of ''BES Cyber System Information,'' or information that could pose a security threat to key industrial control systems for the electric grid. Requirement 2 of Reliability Standard CIP-011-2 requires the responsible entity to ''take action to prevent the unauthorized retrieval of BES Cyber System Information from Cyber Asset data storage media'' prior to disposal or redeployment of such assets. In other words, a generation owner seeking to decommission computer equipment should check to determine whether it contains sensitive information and, if so, should sanitize the storage media of that equipment.

A number of Reliability Standard requirements related to cybersecurity are actually triggered by a decommissioning.

The configuration change management and disposal/redeployment requirements can be overlooked, and NERC has penalized responsible entities for failing to observe these requirements in the context of decommissioning assets. Entities have been fined for not having documented change management procedures (e.g., NERC Violation ID WECC200902147, Find, Fix, Track and Report (July 31, 2013)) or for not abiding by the procedures they do have. E.g., NERC Violation ID MRO201100289, FERC Docket No. NP15-9-000 (Nov. 25, 2014). Similarly, entities have been fined for not taking adequate steps to erase sensitive data from assets that have been taken out of service. NERC Violation ID WECC2015014590, Compliance Exception (Nov. 30, 2015).

A generation owner seeking to decommission control system assets should also make sure that it does not leave any unintended gaps in security. For example,

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

there have been a few cases in which an entity took a device out of service but failed to update firewall settings in accordance with Reliability Standard CIP-005-1 R2. E.g., NERC Violation ID SERC2015014764, Spreadsheet Notice of Penalty, FERC Docket No. NP16-18-000 (April 28, 2016). These failures, in turn, led to firewall ports remaining open when they should have been closed and network traffic routed to devices that no longer were part of the system.

Another possible unintended consequence of a decommissioning is the failure to update required security documentation. For example, NERC has found noncompliance in the following instances:

- Failure to update a Critical Cyber Asset list to reflect the decommissioning of Critical Cyber Assets (CIP-002-1, R3). E.g., NERC Violation ID WECC2015015424, Compliance Exception (July 28, 2016).
- Failure to consider decommissioned assets in the entity's cybersecurity vulnerability assessment (CIP-005-3a, R1). NERC Violation ID SERC2012010737, Spreadsheet Notice of Penalty, FERC Docket No. NP14-14-000 (Dec. 30, 2013).
- Failure to update electronic security perimeter diagrams to reflect changes resulting from the decommissioning of assets (CIP-005-3a, R5). E.g., NERC Violation ID WECC2013012367, Notice of Penalty, Docket No. NP16-5-000 (Nov. 30, 2015).
- Failure to retain electronic access logs associated with the decommissioned assets for ninety days (CIP-005-3a). E.g. NERC Violation ID SERC 2012011380, Notice of Penalty, FERC Docket No. NP14-18-000 (Dec. 30, 2013).

These documentation lapses should not typically pose a significant risk to reliability, and they would likely be caught during the implementation of a robust configuration change management process. Still, even with a robust configuration change management process, major decommissioning projects often prove fertile ground for compliance issues. Often, during a decommissioning, an entity discovers gaps in compliance that it otherwise would not have uncovered. E.g., NERC Violation ID SERC2013012155, Spreadsheet Notice of Penalty, FERC Docket No. NP15-18-000 (Dec. 30, 2014) (finding the virus definition deployment folder of a decommissioned server retained original configuration to allow anonymous access).

Part of the planning process for a plant shut down that entails decommissioning of control systems should include a review of the generation owner's Reliability Standards compliance program. This should begin with a review of the configuration change management process and procedures for disposal and redeployment of control system devices, but it should not end there. Given how integrated the various cybersecurity controls under the Reliability Standards are, it is important to walk through each step in the decommissioning process to understand what actions will need to be taken and when, and the compliance implications of each step.

Ending Compliance Responsibility

The key to understanding when a generation owner's compliance obligations under the Reliability Standards terminate is NERC's compliance registry. The Federal Energy Regulatory Commission (FERC) has made clear that only entities that are on the compliance registry may be penalized for noncompliance with the Reliability Standards. *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, 72 FR 16,416 (Apr. 4, 2007); FERC Stats. & Regs. ¶ 31,242 at 97 (2007) (citations omitted). NERC's procedures for adding and removing entities from the compliance registry are spelled out in the ''Organization Registration and Certification Manual,'' Appendix 5A of NERC's Rules of Procedure.

Unfortunately, the Manual is not well suited to the situation in which a generation owner seeks to decommission a single generating plant. As the title of the Manual suggests, NERC registers entities on an organization-by-organization basis rather than on an asset-by-asset basis. So the manual provides for ''deregistration,'' which would remove an entity completely from the compliance registry, and ''deactivation,'' which would terminate a registered entity's compliance responsibility for a specific function. However, when the generation owner will continue to own other generating plants or to perform other functions that will be covered under the Reliability Standards, the Manual does not provide a good way for a generation owner to sever its compliance responsibility with respect to the one plant it seeks to decommission.

The key to understanding when a generation owner's compliance obligations under the Reliability Standards terminate is North American Electric Reliability Corporation's compliance registry.

Nevertheless, NERC's eight regional entities have developed informal processes to keep track of BES assets owned by registered entities. As part of the registration process, generation owners are required to fill out asset verification forms identifying the generating plants they own. Some of the regional entities explicitly require a generation owner to provide notice of changes to its asset portfolio, such as the decommissioning of a plant. For example, the Northeast Power Coordinating Council (NPCC) states on its Registration page that ''[a] Registered Entity is obligated to notify NPCC upon adding/deleting/transferring equipment, the sale of assets, changes in ownership, or similar matters so that NPCC may review the effect on the Registered Entity's compliance obligations.''

It should be noted that formal ''deactivation'' and ''deregistration''(and presumably less formal notifications to the regional entity of asset retirements) will only serve to cut off compliance responsibilities prospectively. The generation owner will remain responsible for compliance during the period of time that it remained on the compliance registry and the generating plant remained operational.

In short, while NERC's and the regional entities' processes are not perfect, we would recommend that a generation owner seeking to decommission one or more of its generating plants notify its regional entity of such

planned decommissioning. Where applicable, the generation owner may wish to undertake the formal steps to deactivate from the generation function or deregister completely. While such actions will not allow a generation owner to avoid accountability for past noncompliance, they will enable the generation owner to cap off compliance responsibility prospectively.

Personal Information

Personal information is unlikely to be found on the equipment and devices governed by the Reliability Standards. Nevertheless, that does not remove it from regulatory requirements. Instead enterprises must consider the other regulatory regimes that apply. Two predominate: federal rules implemented by the Federal Trade Commission, and state rules that address data security and privacy.

Before discussing those regimes, however, it is necessary to explain ″personal information.″ We use ''personal information'' in a broad sense and mean any information about a person. That information results in data protection obligations when it falls within a state or federal definition. For example, Delaware defines ''Personal Information'' relatively narrowly—a name with a corresponding Social Security number, driver's license number, Delaware ID number or account number with password. 6 Del. Code § 12B-101(4). California, on the other hand, defines ''Personal Information'' more broadly—''any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.'' Cal. Civ. Code § 1798.80(e).

Federal Trade Commission

The Federal Trade Commission (FTC) enforces various laws directed at protecting consumers. Relevant to a utility would be the Fair and Accurate Credit Transactions Act (FACTA), which requires the proper disposal of customer information derived from ''consumer reports'' obtained for a business purpose. 15 U.S.C. § 1681w(a)(1). A ''consumer report'' is defined in the statute to be ''any written, oral, or other communication of any information by a consumer reporting agency,'' which is used or collected for, among other things, credit or employment purposes. 15 U.S.C. § 1681a(d). Any business that obtains a credit check on a consumer or a background check on an employee is subject to the rule. On the basis of this FACTA requirement the FTC promulgated the Disposal Rule, which mandates the proper disposal of such information through ''reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.'' 16 C.F.R. § 682.3(a). Relevant to electronic media, such reasonable measures may include destroying or erasing files containing consumer report information so that the information cannot be read or reconstructed and (after appropriate due diligence) hiring a document destruction contractor. 16 C.F.R. § 682.3(b).

The FTC may also bring enforcement actions based on its authority under section 5 of the FTC Act, which prohibits ''unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.'' 15 U.S.C. § 45(a). Last year the FTC won a substantial victory before the Third Circuit, when the Court of Appeals confirmed that section 5 provides the FTC with authority to pursue enforcement for negligence actions involving consumers' personal information, even without the promulgation of regulations. *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015). (14 PVLR 2228, 12/14/15)

To our knowledge the FTC has not pursued any utilities for improper disposal of consumer information; however, it has not been bashful about going after other business entities. In 2006 an employee of a student loan provider ''sold to the public hard drives that had not been processed to remove the data on the drives.'' FTC, *In re Goal Financial*, Complaint ¶ 6 (April 9, 2008) . While no financial penalty was imposed, the respondent was subject to supervision for over 10 years. *Id.*, Decision and Order (April 9, 2008). There are numerous examples where the FTC pursued businesses for improper disposal of hard copies of consumer information in dumpsters. E.g., *United States v. PLS Fin. Servs., Inc.*, Complaint (N.D. Ill. Oct. 17, 2012) (11 PVLR 1655, 11/12/12). Likewise, the FTC aggressively pursues enterprises whose unencrypted laptops are stolen. FTC, *In re Accretive Health, Inc.*, Complaint (Feb. 5, 2014) (13 PVLR 380, 3/3/14); FTC, *In re Cbr Sys., Inc.*, Complaint (Apr. 29, 2013).

State Data Security Laws

The FTC's jurisdiction extends to information derived from ''consumer reports.'' Employee records not involving a consumer report (e.g., those without a background check or credit report) are not subject to FTC requirements. But state data security and privacy rules very likely will apply. Because there is no overarching federal law in this area, state requirements are a patchwork and must be checked in every jurisdiction.

Improper disposal by a utility of regulated personal information can constitute an actionable breach.

According to the National Conference of State Legislatures, as of Jan. 4, 2016 nearly every American state or territorial jurisdiction has enacted legislation requiring notification of individuals of security breaches of personally identifiable information. NCSL, Security Breach Notification Laws (Jan. 4, 2016). Such laws typically specify who has the compliance obligation, define the scope of ''personal information'', and specify what constitutes a breach and the timing and method required to give notice of the breach. *Id.*

Improper disposal by a utility of regulated personal information can constitute an actionable breach. For example,

- In Illinois a utility disposing of ''materials containing personal information'' must do so in a manner that renders the personal information ''unreadable, unusable, and undecipherable.'' 815 ILCS

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

530/40(b). For electronic media, the statute provides that ''proper disposal methods'' may include destruction or erasure ''so that personal information cannot practicably be read or reconstructed.'' 815 ILCS 530/40(b)(2).

- North Carolina law defines ''Disposal'' as the ''discarding or abandonment of records containing personal information'' or the ''sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal information, . . .'' (N.C. Gen. Stats. § 75-61(7)), North Carolina businesses or entities possessing personal information on North Carolina residents ''must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.'' *Id.* § 75-64(a).

Business Information

The discerning reader will have noted that there is a whole world of information essential to successful operation of a utility that is neither ''personal information'' nor information relevant to the operation of the bulk power system. Such business information—contract terms, fuel prices and other costs, business plans, potential mergers, ramp rates—are of great value to a utility, and to its competitors. Such information is not governed by the Disposal Rule nor by state privacy laws. But even without such outside compulsions, an enterprise's own commercial interests mandate that such information be protected.

Conclusion

Utilities as a whole are a leg up on many industries. The Reliability Standards impose requirements for proper handling and disposal of equipment containing critical operational information. The mindset accompanying compliance with those standards inevitably bleeds over into activities unrelated to the operation of the bulk power system, but which nevertheless have electronically stored information that must be protected. It would surprise us greatly if a NERC-compliant facility did not also have a robust data security program for information (i.e., personal and business information) not subject to NERC requirements.

On shutdown, however, a plant's operational, personal and business information is at risk. The reason is simple: a shutdown plant is no longer a priority. Management's focus is elsewhere, and if that is the case, the old adage: ''you get what you inspect, not what you expect,'' will apply. Without management continuing to take a hard look, even robust programs can stumble. That leads to a very important point in handling electronically stored data in a shutdown plant: do it sooner.

Electronic Data Security Checklist for Shut Down:

- Identify individuals and programs responsible for implementation of plant cybersecurity for operational, personal and business information;
- ensure programs are up-to-date;
- review company's change management and electronic media disposal policies under the relevant programs;
- identify all electronic media and electronic devices that will be affected by plant shut down and information stored on such devices;
- consider whether devices in storage or otherwise unused or redundant can be disposed of or redeployed before shutdown;
- review and update security documentation, including BES Cyber Systems/Assets lists, access privileges, ESP and PSP diagrams, access logs;
- ensure vendors involved in decommissioning and demolition are aware of the need to maintain cybersecurity and capable of doing so;
- advise NERC Regional Entity of plant shut down; and
- be prepared to audit and inspect electronic media disposal.