Report to the

100th General Assembly

Regarding HJR 59

Cybersecurity Task Force

December 2018

Printed by the authority of the State of Illinois
22C-December 2018 - #771

STATE OF ILLINOIS

ILLINOIS COMMERCE COMMISSION

December 19, 2018

The Honorable Members of the Illinois General Assembly
State House
Springfield, Illinois

Dear Honorable Members of the Illinois General Assembly,

House Joint Resolution 59 (hereinafter Resolution or HJR 59) described the threat landscape as of May 2017, created the International Cybersecurity Task Force "Task Force", effective May 31, 2018 and directed the Task Force to submit a final report to the General Assembly by December 31, 2018. The objectives of the Task Force include the following:

1) **Review the Joint Analysis Report** from the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) dated December 29, 2016 **entitled "Grizzly Steppe – Russian Malicious Cyber Activity"** (hereinafter Grizzly Steppe JAR); and 2) **develop strategies to implement or reject recommendations made in the report**; 3) **Make Recommendations to MISO and PJM to insulate Illinois Businesses and Consumers from cyberattacks.**

When HJR 59 was authored in the Spring of 2017, the expectation was that the resulting Task Force would have 18 months to: identify the 27 anticipated members, appoint those members, schedule and conduct a series of meetings, research and summarize the findings of relevant material, agree upon and submit a final report to the General Assembly of its findings by the end of 2018 and thereby officially dissolve the Task Force. Although the Resolution was adopted by the House on June 22, 2017, it was not adopted by the Senate until May 31, 2018. As a result, a significantly truncated timeline remained for the Task Force to organize and attempt to meet the objectives outlined in the Resolution.

A Chair, Co-Chair and the anticipated Task Force members were not appointed during the remaining truncated timeline. Because the Resolution directed (the anticipated Task Force) to be created within the Illinois Commerce Commission ("ICC") by the appointees, the ICC's Director of Cybersecurity and Risk Management, who specializes in this subject matter on behalf of the ICC, recommends that the General Assembly accept the timely delivered accompanying report on behalf of and in lieu of the contemplated Task Force report. The submitted report ("A Report to the General Assembly") was created by the ICC through its Director of Cybersecurity and Risk

Management in a manner that addresses the original goals and content objectives of the Resolution.

Should the 101st General Assembly determine it is appropriate for a new or replacement Task Force to be created, any such resulting Task Force will have this Report available as a resource for its appointees to assist with determining the best course of action moving forward. If the General Assembly chooses to create a new task force, sufficient time should be given to its appointees to organize, meet, research, discuss, draft and submit a report. It is anticipated that a minimum of 12-18 months would be needed to address objectives similar to those described in HJR 59.

Alternatively, the General Assembly may accept this report as the finished product meeting the full objectives of the Resolution, on behalf of the proposed Task Force and those members who sponsored the Resolution.

Should you have questions about the enclosed Report, please contact Michelle Kelm, ICC Director of Governmental Affairs, at (217) 524-0619.

Sincerely,

Dominic Saebeler
Director of Cybersecurity and Risk Management
Illinois Commerce Commission

Note: This Report to the General Assembly may also be accessed on the Illinois Commerce Commission's webpage at www.icc.illinois.gov/reports. Many of the report footnotes contain active hyperlinks to outside referenced sources. For those applicable footnotes, when reviewing this report electronically, simply move your cursor over the citation and click to be redirected to the original referenced source.

A Report to the General Assembly

This report is in satisfaction of the requirements of House Joint Resolution 59 of the 100th General Assembly

House Joint Resolution 59

The 100th General Assembly's House Joint Resolution 59 (hereinafter Resolution or HJR 59) created the International Cybersecurity Task Force ("Task Force"), effective May 31, 2018. The objectives of the Resolution include the following:

a) Describe the threat landscape during May of 2017;
b) Direct the creation of the Task Force within the Illinois Commerce Commission;
c) Review the Joint Analysis Report from the U.S. Department of Homeland Security ("DHS") and the Federal Bureau of Investigation ("FBI") dated December 29, 2016 entitled "Grizzly Steppe – Russian Malicious Cyber Activity" ("Grizzly Steppe JAR") and develop strategies to implement or reject recommendations made in the report;
d) Make Recommendations to MISO and PJM to insulate Illinois Businesses and Consumers from cyberattacks;
e) Make a report to General Assembly by December 31, 2018;
f) Dissolve the Task Force upon report submission.

Analysis and Approach to Addressing Objectives

Although not the result of a fully formed International Cybersecurity Task Force ("Task Force") as contemplated by HJR 59 (the "Resolution"), this Report does fully address the above objectives of the Joint Resolution. The Resolution directed creation of the Task Force within the Illinois Commerce Commission ("ICC"). Because of a truncated timeline (less than 6 months) resulting from a one-year gap between adoption of HJR 59 by the Illinois House (in June of 2017) and the subsequent Senate adoption (on May 31, 2018), this report was created by the ICC through its Director of Cybersecurity and Risk Management who specializes in this subject matter. This Report is thereby provided on behalf of the International Cybersecurity Task Force by the ICC to timely report on and achieve the objectives of the Resolution.

Threat Environment in Early 2017 and Today

The threat landscape described within the Resolution was accurate for early 2017. Much has changed and evolved since the Grizzly Steppe JAR was issued. New threats emerge, and as response tactics evolve and disruption prevention strategies change, the recommendations and reactions prevalent at that time should be revisited 17 months later.

The May 2017 WannaCry ransomware attack contemplated by the Resolution impacted entities in many different sectors worldwide. One of the hardest hit organizations was the National Health Service in the United Kingdom, which had to cancel at least 6,900 patient appointments, including surgical procedures.[1] More than 1/3 of healthcare organizations under the system were affected by the malware, which disrupted access to patient records, test results, and prescription and fulfillment.[2] In June 2017, entities in Ukraine, including the electric utilities, suffered attacks from similar malware variant called "NotPetya". In December 2017, the United States and the UK attributed the WannaCry attack to North Korea, raising "public awareness about North Korea's growing offensive cyber capabilities."[3] In February 2018, the United States and the UK attributed the NotPetya attack to Russia.[4] These attacks hold data as ransom, and are different in kind from campaigns aimed at gaining the ability to cause physical disruptions on the grid. Such campaigns target supervisory control and data acquisition (SCADA) systems, which are the most commonly used form of industrial control systems (ICS). These systems are also referred to as operational technologies (OT). These OT systems are generally segmented from the information technology (IT) systems that support common business functions. Ransomware is typically not considered a primary threat to grid reliability and resilience as ransomware attacks like WannaCry appear to target IT systems, rather than OT systems. However, introduction and utilization of all advanced technologies must be accompanied by a continuous assessment of necessary security related costs.

Since the release of the Grizzly Steppe JAR contemplated by the Resolution, several high profile cyber incidents have redirected the attention of cybersecurity practitioners. In September 2017, DHS issued a binding operational directive that ordered removal of all Kaspersky products from federal government computing assets, citing concerns over "[t]he risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates US national security."[5] In October 2017, the DHS and the FBI released a joint Technical Alert (TA17-293A) detailing the Dragonfly campaign: "advanced persistent threat (APT) actions targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors" since at least 2015.[6] In late

---

[1] *NHS "could have prevented" WannaCry ransomware attack*, BBC (Oct. 27, 2017), http://www.bbc.com/news/technology-41753022.

[2] *NHS cyber-attack: GPs and hospitals hit by ransomware*, BBC (May 13, 2017), http://www.bbc.com/news/health-39899646.

[3] Thomas P Bossert, *It's Official: North Korea Is Behind WannaCry*, WASH. POST (Dec. 18, 2017), https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

[4] *UK and US blame Russia for 'malicious' NotPetya cyber-attack*, BBC (Feb. 15, 2018), https://www.bbc.com/news/uk-politics-43062113.

[5] Joe Mullin, *Kaspersky software banned from US government agencies*, ARS TECHNICA (Sept. 13, 2017, 2:35 PM), https://arstechnica.com/tech-policy/2017/09/kaspersky-software-banned-from-us-government-agencies.

[6] *Alert (TA17-293A)*, US-CERT (Oct. 20, 2017) [hereinafter TA17-293A], https://www.us-cert.gov/ncas/alerts/TA17-293A.

December 2017, in the first reported incident of a breach affecting the safety systems at an industrial plant, security researchers shared the discovery of a Windows-based malware named Triton.[7] Researchers later discovered the attack was intended to cause physical damage at the targeted petrochemical plant, and the "only thing that prevented an explosion was a mistake in the attackers' computer code."[8]

In January 2018, researchers reported on a hacking group dubbed Dark Caracal that has been traced to the Lebanese intelligence agency, with evidence of attacks by this group found on government agencies, militaries, defense contractors, utilities, enterprises, and financial institutions spanning more than 21 countries. A relatively new technique used by this group is trojanized applications on mobile devices.[9]

In March 2018, a joint Technical Alert (TA18-074A) follow up to the October 2017 Alert (TA17-293A) released by the DHS and the FBI attributed responsibility to Russia for the ongoing Dragonfly campaign against "U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[10] This ongoing campaign gained additional attention in July 2018 through a series of DHS NCCIC briefings. Starting in May 2018, various entities in the U.S. government took steps against ZTE and Huawei, technology firms based in the People's Republic of China, due to concerns over cyber supply chain security. In August 2018, cybersecurity firms reported on a hacking group called Raspite, possibly based in Iran, targeting industrial control systems in U.S. electric utilities.[11]

The preceding incidents have arguably refined and redirected the focus of critical infrastructure defenders away from ransomware-based attacks and broader malicious cyber activities of the entities named in the Grizzly Steppe JAR (APT 28 and APT 29). Instead, the focus has shifted towards activities that present more immediate threats to grid cyber security such as ICS focused attacks. In fact, the DHS and the FBI have since released new information regarding malicious activities referred to as Grizzly Steppe as focus shifts from ransomware (TA17-181A,[12]

---

[7] Andy Greenberg, *Unprecedented Malware Targets Industrial Safety Systems in the Middle East*, WIRED (Dec.14, 2017 10:00 AM), https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east.

[8] Nicole Perlroth & Clifford Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

[9] EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World, EFF (Jan. 18, 2018), https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around.

[10] *Alert (TA18-074A)*, US-CERT (Mar. 15, 2018) [hereinafter TA18-074A], https://www.us-cert.gov/ncas/alerts/TA18-074A.

[11] Andrew Blake, *U.S. electric utilities targeted by suspected state-sponsored hacking group, security firm warns*, WASH. TIMES (Aug. 2, 2018), https://www.washingtontimes.com/news/2018/aug/2/us-electric-utilities-targeted-suspected-state-spo/.

[12] *Alert (17-181A)*, US-CERT (July 1, 2017) [hereinafter TA17-181A], https://www.us-cert.gov/ncas/alerts/TA17-181A.

February 15, 2018 Technical Alert – Petya Ransomware), to energy and other critical infrastructure (TA18-074A, March 15, 2018 Technical Alert Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors), [13] and network infrastructure devices (TA18-106A, April 16, 2018 Technical Alert – Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices). [14] However, many of the recommendations from the Grizzly Steppe JAR are generally applicable and constitute best practices that should be followed.

Recommendation to Municipal and Local Government

The Resolution contemplates inclusion of five Illinois mayors as members of the proposed Task Force. Though mayors of major cities in Illinois have a smaller geographic footprint, they are typically more closely connected with key decision making that relates to important utility cybersecurity investments. Cities across Illinois are facing critical decisions related to securing local infrastructure. Mayors will set the tone for ongoing partnering, engagement, communication and coordination with both municipal utilities and co-operatives as well as local, state and federal first responders. Informed mayors, who both understand the risks and prioritize a strategic balancing of resources can have a tremendous positive impact on protecting the assets that are connected to the grid across the state. As important as their involvement is, municipal and local governments may not have the same level of resources that an investor owned utility possesses. Prioritizing access to and allocation of resources (including skilled staff) is critical when considering the best approach to fostering a unified effort that ensures reliability, resiliency and the overall security of utilities across the state of Illinois. The businesses in Illinois rely on consistent availability of services provided by all utilities.

Though the potential inclusion of and perspective from local leaders is important when analyzing exiting cyber threats to critical infrastructure, the recommendations contained in Grizzly Steppe JAR do not focus on the role of state and local leaders. The role of local authorities should include gaining access to and implementing the same recognized best practices that are developed across the industry and country. Where resource challenges exist, mayors can weigh in on the necessity of achieving minimum levels of security across local utilities. While the Grizzly Steppe JAR analyzes a broad set of risks and proposed disciplines the underlying recommendations are not tailored towards specific subset of entities. That is, these recommendations are scalable for jurisdictions of all sizes, including local, state, and federal entities as well as businesses and individuals. Local governments should take the necessary steps to regularly engage municipal utility entities, co-operatives, investor owned utilities, and any other utility service providing entity they regularly interact with or have jurisdiction over.

[13] TA18-074A.

[14] Alert (TA18-106A), US-CERT (April 16, 2018) [hereinafter TA18-106A], https://www.us-cert.gov/ncas/alerts/TA18-106A.

Summary of Grizzly Steppe Report

In December 2016, the National Cybersecurity & Communications Integration Center (NCCIC) released a Joint Analysis Report titled "GRIZZLY STEPPE – Russian Malicious Cyber Activity) (JAR-16-20296A). This analytic effort by DHS and FBI details tools and infrastructure used by Russian civilian and military intelligence services in activities against government, critical infrastructure entities, think tanks, universities, and political organizations.

The Grizzly Steppe JAR details how the threat actors delivered malware to systems, established persistence, escalated privileges, and exfiltrated information. Delivery of malware (malicious software intended to damage or disable) to gain initial foothold in target organizations was accomplished through spear phishing (malicious email targeted towards specific individuals often ostensibly from a known or trusted sender) containing malicious links and tricking targets into clicking on the links, taking certain actions such as making monetary transfers, and/or disclosing credentials or other sensitive information. In preparation for hosting malware and sending phishing emails, the attackers gained access to and established control of legitimate domains associated with U.S. organizations.

Analysis of Recommended Mitigations

One or more cyber-attacks on the grid have the potential to negatively impact the grid in some capacity (there is ongoing disagreement as to the degree of potential impact), the result could be significant to the people and economy of Illinois. The Investor Owned, Co-Operative and Municipal Electric utilities are aware of the Grizzly Steppe JAR and the recommendations contained therein. The industry is in general agreement with the Grizzly Steppe JAR's recommendations. However, almost two years have passed and new and emerging threats have occurred since the Grizzly Steppe JAR as the threat landscape continuously evolves. The content of the Grizzly Steppe JAR is arguably dated,[15] and focus of cybersecurity has shifted to new and emerging threats.

Most mitigations in the Grizzly Steppe JAR, however, are generally applicable and should nevertheless be implemented by all network administrators.[16] This report recognizes that no two environments are the same and there may be idiosyncratic reasons a specific mitigation may be more harmful than good in a specific environment. At this point, most utilities have likely implemented most or all of the appropriate recommendations. However, the following modifications should be considered when using the Grizzly Steppe JAR as a basis for developing strategies, informing the public, and making recommendations for actions to be taken.

[15] Leonid Bershidsky, *U.S. Intelligence Got the Wrong Cyber Bear*, BLOOMBERG (Jan. 2, 2017) https://www.bloomberg.com/view/articles/2017-01-02/u-s-intelligence-got-the-wrong-cyber-bear.
[16] Ira Winkler, *Making the GRIZZLY STEPPE Joint Action Report useful*, CSO (Jan. 9 2017) https://www.csoonline.com/article/3155754/data-breach/making-the-grizzly-steppe-joint-action-report-useful.html.

Recommended Mitigations

The Grizzly Steppe JAR recommendations are separated into three broad categories, "**Commit to Cybersecurity Best Practices**," "**Top Seven Mitigation Strategies**," and "**Responding to Unauthorized Access to Networks**." The Grizzly Steppe JAR's Recommendations can be further separated into two categories: **Prevention** and **Preparedness**. Prevention activities include risk analysis, vulnerability scanning and patching, penetration testing, application whitelisting, network segmentation, server vulnerability mitigation, firewall configuration, restrict privileges, and staff training. Preparedness activities include backups, Incident response, and business continuity. Lastly, the Grizzly Steppe JAR points to many useful resources from DHS and other organizations; for example, Cyber Security Advisors (CSA) program, Cyber Resilience Review (CRR), Enhanced Cybersecurity Services (ECS), The Cybersecurity Information Sharing and Collaboration Program (CISCP), The Automated Indicator Sharing (AIS), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). For a comprehensive explanation of the above, see www.dhs.gov.

The recommendations are summarized here as a list. For detailed explanations, see the Grizzly Steppe JAR at https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Commit to Cybersecurity Best Practices

1. Backups
2. Risk analysis
3. Staff training
4. Vulnerability scanning & patching
5. Application whitelisting
6. Incident response
7. Business continuity
8. Penetration testing

Top Seven Mitigation Strategies

1. Patch applications and operating systems
2. Application whitelisting
3. Restrict administrative privileges
4. Network segmentation and segregation into security zones
5. Input validation
6. File reputation
7. Understanding firewalls

Responding to Unauthorized Access to Networks

1. Implement your security incident response and business continuity plan.
2. Contact DHS or law enforcement immediately.

Detailed Mitigation

The Grizzly Steppe JAR also includes detailed mitigation strategies, providing mitigations against specific threats. The following analysis is intended for those personnel responsible for cybersecurity strategy, implementation, and tactical execution at various critical infrastructure entities. Those responsible for policy decisions should discuss the applicability of Grizzly Steppe JAR recommendations with the cybersecurity personnel.

Protect Against SQL Injection and Other Attacks on Web Services

1. Routinely evaluate known and published vulnerabilities
2. Perform software updates and technology refreshes periodically
3. Audit external-facing systems for known Web application vulnerabilities.
4. Harden both Web applications and the servers hosting them to reduce the risk of network intrusion
5. Use and configure available firewalls to block attacks.
6. Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
7. Monitor and remove any unauthorized code present in any www directories.
8. Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) and response to these protocols as much as possible.
9. Remove non-required HTTP verbs from Web servers as typical Web servers and applications only require GET, POST, and HEAD.
10. Where possible, minimize server fingerprinting by configuring Web servers to avoid responding with banners identifying the server software and version number.
11. Secure both the operating system and the application.
12. Update and patch production servers regularly.
13. Disable potentially harmful SQL-stored procedure calls.
14. Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
15. Consider using type-safe stored procedures and prepared statements.
16. Perform regular audits of transaction logs for suspicious activity.
17. Perform penetration testing against Web services.
18. Ensure error messages are generic and do not expose too much information.

Phishing and Spear phishing

1. Implement a Sender Policy Framework (SPF) record for your organization's Domain Name System (DNS) zone file to minimize risks relating to the receipt of spoofed messages.
2. Educate users to be suspicious of unsolicited phone calls, social media interactions, or email messages from individuals asking about employees or other internal information.

Should an unknown individual claim to be from a legitimate organization, try to verify his or her identity directly with the company.

3. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
4. Do not reveal personal or financial information in social media or email, and do not respond to solicitations for this information. This includes following links sent in email.
5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL often includes a variation in spelling or a different domain than the valid website (e.g., .com vs. .net).
6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
7. Take advantage of anti-phishing features offered by your email client and web browser.
8. Patch all systems for critical vulnerabilities, prioritizing timely patching of software that processes Internet data, such as web browsers, browser plugins, and document readers.

Permissions, Privileges, and Access Controls

1. Reduce privileges to only those needed for a user's duties.
2. Restrict users' ability (permissions) to install and run unwanted software applications and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
3. Carefully consider the risks before granting administrative rights to users on their own machines.
4. Scrub and verify all administrator accounts regularly.
5. Configure Group Policy to restrict all users to only one login session, where possible.
6. Enforce secure network authentication where possible.
7. Instruct administrators to use non-privileged accounts for standard functions such as Web browsing or checking Web mail.
8. Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
9. Configure firewalls to disallow RDP traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary VPN with lower privileges.
10. Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.

11. Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. This can be indicative of failed intrusion activity.
12. If remote access between zones is an unavoidable business need, log and monitor these connections closely.
13. In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

Credentials

1. Enforce a tiered administrative model with dedicated administrator workstations and separate administrative accounts that are used exclusively for each tier to prevent tools, such as Mimikatz, for credential theft from harvesting domain-level credentials.
2. Implement multi-factor authentication (e.g., smart cards) or at minimum ensure users choose complex passwords that change regularly.
3. Be aware that some services (e.g., FTP, telnet, and .rlogin) transmit user credentials in clear text. Minimize the use of these services where possible or consider more secure alternatives.
4. Properly secure password files by making hashed passwords more difficult to acquire. Password hashes can be cracked within seconds using freely available tools. Consider restricting access to sensitive password hashes by using a shadow password file or equivalent on UNIX systems.
5. Replace or modify services so all user credentials are passed through an encrypted channel.
6. Avoid password policies that reduce the overall strength of credentials. Policies to avoid include lack of password expiration date, lack of lockout policy, low or disabled password complexity requirements, and password history set to zero.
7. Ensure that users are not re-using passwords between zones by setting policies and conducting regular audits.
8. Use unique passwords for local accounts for each device.

Logging Practices

1. Ensure event logging (applications, events, login activities, security attributes, etc.) is turned on or monitored for identification of security issues.
2. Configure network logs to provide enough information to assist in quickly developing an accurate determination of a security incident.
3. Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
4. Secure logs, potentially in a centralized location, and protect them from modification.
5. Prepare an incident response plan that can be rapidly implemented in case of a cyber intrusion.

Modifications and Further Discussion of Specific Recommendations Contained in the Grizzly Steppe JAR

Utilization of the elements in the above list will likely be modified to suit the unique environments of each entity. The following analysis addresses some generally applicable recommended modifications of elements in the Grizzly Steppe JAR that may be appropriate in many environments.

***Use and configure available firewalls to block attacks*:** should be restated to "use and configure firewalls to only allow legitimate traffic." This is not a pedantic or purely semantic distinction. The assumption in firewall configurations should be to only allow legitimate traffic, not just to block illegitimate traffic. In addition, it is unnecessary to specify use and configuration of only "available" firewalls. In fact, where firewalls are needed and unavailable, they should be made available. In addition, the assumption in firewall configurations should be to only allow legitimate traffic, not to block illegitimate traffic.

Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker: Additionally, similar steps should be taken to secure other operating systems, if present, to allow execution of only authorized applications. Network environments often include a mixture of different operating systems.

Application whitelisting: whitelisting has been challenging in some environments due to the administrative complexity. This report recommends that additional study should be conducted to ascertain the feasibility of deploying application whitelisting (1) organization wide or (2) in high impact segments such as the operational networks of the grid. Application whitelisting may be the best path forward, particularly in environments with high security requirements and limited and predictable software changes. File reputation checks can be used as a less aggressive alternative or interim solution while the feasibility studies for deployment of application whitelisting are underway. In place of application whitelisting, file reputation sub-systems of antivirus systems can be tuned to allow execution of only the highest reputation files.

Update and patch production servers regularly: as a recommended strategy to protect against attacks on web services, the Grizzly Steppe JAR recommends that production servers should be updated and patched regularly. While that is sensible, it should be explicitly stated and clarified that before patches are applied to assets in the production environment, updates and patches must be thoroughly tested in a testing environment that simulates the production environment to ensure they will not cause unintended changes in functionality or, worse, disruptions.

***Sanitizing and validating input, use of parametrized queries (prepared statements)*:** administrators and developers should also employ "consistent and proper use of syntax and language functions to safely escape special characters that might be present in user input."[17]

Protection against malicious URLs that include misspelling or different TLD: in addition, both user training and technical mitigation actions should also contemplate homograph attacks using Unicode characters that are difficult to distinguish from common ASCII characters.[18] These malicious URLs direct users to webservers under the control of the attackers by tricking users into visiting websites with URLs that, upon first inspection, appears to match that of the legitimate resources. Misspelled URL attacks take advantage of typographical errors or spelling errors (e.g. *illinois.gov* versus *ilinois.gov*, the latter having one "*l*" instead of two). TLD, or top-level domain, refers to the highest level in the Domain Name System, represented by the last part of the domain name (e.g. *.com, .net, .edu, .gov*). A TLD attack uses a site registered to a domain with the same name but on a different TLD (e.g. *illinois.gov* versus *illinois.com*). Lastly, homograph attacks use similar looking characters to replace characters in the legitimate domain name (e.g. *illinois.gov* versus *i1linois.gov*, with a "*1*" replacing the "*l*".) Font selection will have a significant impact on the readers' ability to identify this subtle difference; Another example would be (*illinois.gov* versus *illinois.gov)* with the latter "*i*" replaced by a Cyrillic counterpart, which is practically indistinguishable regardless of font.

Reducing privileges to only those needed for a user's duties, applying the principle of "Least Privilege": in addition, entities should consider limiting use of administrative privileges only at the time the user is performing those duties. While the Grizzly Steppe JAR recommends instructing administrators to use non-privileged accounts for standard functions, this report recommends that the recommendation be stated in a different manner. That is, administrators should be instructed to always use a standard user account except when performing administrative duties; administrators should limit use of administrator accounts to only when absolutely necessary to performing administrative duties.[19]

***Carefully consider the risks before granting administrative rights to users on their own machines*:** and only grant administrative privileges to users on their own machines where absolutely necessary and all alternatives would unreasonably hinder business processes.

Firewall rules should be audited to close all ports that are not explicitly needed for business: instead, this should be restated as "all firewall rules should be audited to only allow ports explicitly needed for specific business functions." As stated above, the best practice in firewall

---

[17] *Injection Prevention Cheat Sheet*, OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (Nov. 25, 2017), https://www.owasp.org/index.php/Injection_Prevention_Cheat_Sheet#Injection_Prevention_Rules.

[18] Alex Hern, *Unicode trick lets hackers hide phishing URLs*, GUARDIAN (Apr. 2017), https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers.

[19] *Compare* privilege bracketing in software development, which utilizes temporary increase in software privilege to perform a specific function.

configurations should be to only allow legitimate traffic, not just to block illegitimate traffic. Other aspects of network traffic flow should also be controlled in general, in addition to ports.

All users be restricted to one login session: this recommendation can be strengthened by monitoring, logging, and reviewing login attempts and geographic location. Moreover, entities should consider deploying technologies and procedures to resolve physical authentication (e.g. keycard access) with digital access to identify unusual activities. This can be helpful in identifying malicious access attempts if there is an unusual mismatch between the user's purported physical location and digital access attempts.

Ensuring users use complex passwords and enforcing frequent password expiration: this recommendation is long practiced by system administrators. However, NIST Special Publication 800-63 Digital Identity Guidelines[20] on memorized secrets usability considerations now recommends requiring a lengthy password with few other complexity requirements, not requiring arbitrary periodic changes unless requested or there is evidence of compromise, and facilitating the use of password managers.[21] Arbitrary periodic changes and complexity requirements may inadvertently increase unsecure user behavior such as writing down passwords or using iterations of the same password with minimal changes. This report also recommends use of multifactor authentication wherever feasible.

Minimizing use of services that transmit user credentials in clear text, such as FTP and telnet, or moving to more secure alternatives: In addition, administrators can also consider, in the interim, mitigations such as retrofitting to encapsulate the clear text traffic in encryption at either end, and only decrypting at the last moment as required by legacy systems.[22]

Entities should ensure event logging is turned on or monitored: this report recommends that event logging is enabled and monitored.

Lastly, this report recommends adding the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and the DHS National Risk Management Center (NRMC) to the *resources list*. DOE CESER focuses on cybersecurity for critical energy infrastructure: (1) Strengthening energy sector cybersecurity preparedness (2) Coordinating cyber incident response and recovery and (3) Accelerating research, development and demonstration (RD&D) of game-changing and resilient energy delivery systems. The DHS NRMC will serve as a "one stop shop" for local, state, federal, and private organizations in a cybersecurity crisis.

Analysis of MISO PJM roles

The Resolution instructs the Task Force to review the Grizzly Steppe JAR and "develop strategies to either implement or reject the recommendations made in the report", and "make

[20] *Digital Identity Guidelines*, NAT'L INST. OF STANDARDS & TECH. (June 22, 2017), https://pages.nist.gov/800-63-3/.
[21] Paul A. Grassi et al., NAT'L INST. OF STANDARDS & TECH., Special Publication 800-63B, https://doi.org/10.6028/NIST.SP.800-63b.
[22] Such as by using "bump-in-the-wire" devices.

recommendations to [MISO] and PJM . . . relative to insulation of Illinois businesses and consumers from cyberattacks."

"Wholesale physical power trade typically occurs through bilateral transactions, and while the industry had historically traded electricity through bilateral transactions and power pool agreements, Order No. 888 promoted the concept of independent system operators (ISOs)."[23] ISOs operate the transmission system, foster competition for electric generation among wholesale market participants, and facilitate open access to electric transmission.[24] Wholesale electricity markets facilitate open-access to transmission.

MISO and PJM manage and coordinate wholesale electricity in their respective footprints.[25] They are independent organizations that match supply and demand of energy and improve market efficiency and grid reliability day to day, as well as identify efficient and cost effective long-term improvements to the grid.[26] MISO and PJM also perform outage coordination and restoration.[27] While the trend towards increasing DER integration has some associated security concerns for the wholesale markets, it is unclear whether MISO and PJM would currently be the best institutions to insulate Illinois businesses and consumers from cyberattacks. However, they could have a role in insulating Illinois businesses and consumers from the *effects* of cyberattacks on the electric grid.

These market operators work with members and partners to "exchange information, leverage existing expertise, and share tools, capabilities, and resources [to put] everyone in a stronger position to prepare for and defend against attacks and minimize disruptions."[28] The industry has converged towards following the NIST Cybersecurity Framework (CSF) for standards and best practices to manage cybersecurity risks. MISO and PJM's priority is fortifying its own systems, detecting adverse events, and responding and recovering from events.[29] MISO and PJM work with government, industry, and other CI in collaborative efforts to share expertise

[23] *Electric Power Markets: National Overview*, FERC, https://www.ferc.gov/market-oversight/mkt-electric/overview.asp.
[24] *Id.*
[25] *Reliability Operating Procedures*, MISO, https://www.misoenergy.org/markets-and-operations/reliability-operating-procedures/; *Who We Are*, PJM, http://www.pjm.com/about-pjm/who-we-are.aspx.
[26] *Id.*
[27] *Markets and Operations*, MISO, https://www.misoenergy.org/markets-and-operations/.
[28] *New Learning Center page highlights cybersecurity, safeguarding the grid*, PJM (March 19, 2018) http://insidelines.pjm.com/new-learning-center-page-highlights-cybersecurity-safeguarding-the-grid/; Press Release, MISO, *MISO: Grid resilience is core to our foundation* (March 9, 2018), https://www.misoenergy.org/about/media-center/miso-statement-on-ferc-resilience-filing/.
[29] *Safeguarding the Grid*, PJM, https://learn.pjm.com/three-priorities/keeping-the-lights-on/safeguarding-the-grid.aspx; MISO MARKET SYSTEM EVALUATION, MISO (Sep. 11, 2017), https://cdn.misoenergy.org/MSE_Final%20Report_Public140327.pdf.

and improve cyber and physical security, including simulations, exercises, and training.[30] Prominent entities facilitating these collaborative efforts include the Electricity Subsector Coordinating Council (ESCC), the Electricity Information Sharing and Analysis Center (E-ISAC), DHS, DOE, FERC, FBI, and DoD.

NERC Reliability Standards are mandated by FERC and developed by NERC to define the requirements followed by those operating the North American bulk power system. The standards are followed and enforceable against all those entities. PJM and MISO also participate in the development of those reliability standards.[31] In addition, PJM and MISO are encouraged to participate collaboratively in the development of emergency operations plans with federal regulators. These plans may include options, in response to anticipated or ongoing cyber-based disruptions, for (1) operating above the maximum economic levels if additional reserve margins are needed, (2) suspending wholesale market operations, or (3) halting service to or islanding areas preemptively to minimize damage.[32]

MISO and PJM, like the rest of the industry, are keenly awareness of the issue, and have taken steps toward insulating businesses and consumers from cyber-attack impact where possible. We recommend MISO and PJM continue collaborative efforts with industry stakeholders to protect the BES and consequently protect Illinoisans. To the extent MISO and PJM have specific recommendations that can be taken to insulate Illinois businesses and consumers from cyberattacks, they are encouraged to share those through the appropriate channels.

Conclusion

In summary, the recommendations of the Joint Analysis Report from the U.S. Department of Homeland Security and Federal Bureau of Investigation dated December 29, 2016 entitled "Grizzly Steppe – Russian Malicious Cyber Activity" contains a significant amount of important information that can be used productively to inform the behavior of those responsible for protecting critical infrastructure in Illinois. The Joint Analysis Report is also a useful general guide to appropriate behaviors, safe cyber practices and proactive tactical steps that can be taken to prevent unauthorized access to operational systems.

The threat landscape captured in the Resolution is accurate for the Spring 2017 timeframe. Much has changed and evolved since the referenced incident and report. New threats emerge and as threat actors' tactics evolve, so must the tactics of those defending the grid. Evidence supports the fact that hostile nation states are actively attempting to penetrate U.S. critical infrastructure. It should be expected that Illinois infrastructure is included in those efforts.

---

[30] *Safeguarding the Grid*, PJM, https://learn.pjm.com/three-priorities/keeping-the-lights-on/safeguarding-the-grid.aspx; MISO, *MISO: Grid resilience is core to our foundation* (March 9, 2018), https://www.misoenergy.org/about/media-center/miso-statement-on-ferc-resilience-filing/.

[31] *See e.g. Murphy discusses role on NERC supply chain cybersecurity standards team*, MISO, http://insidelines.pjm.com/murphy-discusses-role-on-nerc-supply-chain-cybersecurity-standards-team/.

[32] Paul N. Stockton, *Resilience for Grid Security Emergencies*, JOHNS HOPKINS APPLIED PHYSICS LABORATORY (2018), http://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf.

Continuous diligence toward protecting Illinois infrastructure is necessary. As a result, ongoing support for programs that promote reasonable cybersecurity focused efforts, adoption of best practices and strategic investments in enhancing efforts to protect critical infrastructure is and will be needed today and continuously moving forward. A general recognition that active cybersecurity programs and defense measures have become a necessary component of risk awareness and mitigation efforts across industries, businesses and governments is of paramount importance.

While recommendations to MISO and PJM have been suggested, the current role of ISOs like MISO and PJM is not necessarily to inform, direct or insulate Illinois businesses and consumers from cyber-attacks. Instead, ISOs work collaboratively with stakeholders to improve cyber security capabilities of portions of the bulk electric system serving the respective regions. Through its direct impact of the strategic and economic operation of the grid, an ISO does play a significant role in protecting a key component of Illinois' critical infrastructure. These ISOs should also be available to collaborate with and jointly assess any overlap in critical infrastructure cyber defense strategies to ensure the grid is reliable, resilient and secure.

While much has been accomplished since the Grizzly Steppe JAR was first issued, much more is left to be done. In addition to considering recommendations contained within the JAR, Illinois business and government leaders should continue to emphasize and support a risk-based approach that includes awareness, minimizing threat vectors where possible, organizational competency and a combined focus on prevention and consistent best practice adoption. Allocation of resources toward mitigating those threats that have the greatest likelihood of negative consumer, financial, and system and impact is appropriate and should be a foundational component of cyber risk mitigation strategies and investment decisions.

While the objectives of the Resolution and thereby the Task Force have been met by this report, it is advisable that this topic be regularly assessed, and industry experts consulted as to what actions will be necessary going forward to most effectively address this evolving threat continuum.

By:

Dominic Saebeler, Director of Cybersecurity and Risk Management

Wei Chen Lin, Policy Advisor, Office of Cybersecurity and Risk Management

Illinois Commerce Commission