ICS-CERT INFORMATION BULLETIN

ICSB-11-327-01—ILLINOIS WATER PUMP FAILURE REPORT

November 23, 2011

REPORT

On November 10, 2011 the Illinois Statewide Terrorism & Intelligence Center (STIC) issued a Daily Intelligence Notes report entitled "Public Water District Cyber Intrusion." As widely reported in the press, the report detailed initial findings of anomalous behavior in a supervisory control and data acquisition (SCADA) system at a Central Illinois public water district. This report also alleged a malicious cyber intrusion from an IP address located in Russia that caused the SCADA system to power on and off, resulting in a water pump burn out.

ICS-CERT was made aware of the report on November 16, 2011, and immediately reached out to the STIC to gather additional information. ICS-CERT was provided with a log file; however, initial analysis could not validate any evidence to support the assertion that a cyber intrusion had occurred.

ICS-CERT reached out to the affected entity, Curran-Gardner Public Water District, to gather detailed information and offer support and analytics to uncover what caused the pump to fail[1]. At the request of the utility and in coordination with the FBI, ICS-CERT deployed a fly-away team to the facility to interview personnel, perform physical inspections, and collect logs and artifacts for analysis.

After detailed analysis of all available data, ICS-CERT and the FBI found no evidence of a cyber intrusion into the SCADA system of the Curran-Gardner Public Water District in Springfield, Illinois.

In addition, there is no evidence to support claims made in the initial Illinois STIC report – which was based on raw, unconfirmed data and subsequently leaked to the media – that any credentials were stolen, or that the vendor was involved in any malicious activity that led to a pump failure at the water plant. In addition, DHS and the FBI have concluded that there was no malicious or unauthorized traffic from Russia or any foreign entities, as previously reported.

Analysis of what caused the pump to fail is ongoing. ICS-CERT will continue to coordinate with the FBI, Water ISAC, MS-ISAC and other organizations as appropriate.

Publicly disclosing affected identity names with incident information is highly unusual and not part of ICS-CERT's normal incident reporting and triage procedures. In this particular case, because unconfirmed information had already been leaked to the public, ICS-CERT and the asset owner/operator

[1] Note: At no time were there any impacts to customers served by the water district due to the pump failure.

felt it was in the best interest of the community to collaboratively analyze all available data and disclose some of the findings. ICS-CERT would like to thank the Curran-Gardner Public Water District and the SCADA systems integrator (vendor) for their cooperativeness in pulling all available resources in order to conduct a thorough and exhaustive investigation. It is our hope that this information will inform the community and help to quell some of the wide speculation that has ensued in the media.

At this time, there are no specific recommendations other than to ensure you are following security best practices. ICS-CERT recommends reviewing *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies* for more information.

ICS-CERT encourages those in the industrial control systems community who suspect or detect any malicious activity against/involving control systems to contact ICS-CERT for assistance and tracking. ICS-CERT works with organizations to protect their data, including leveraging the Protective Critical Infrastructure Information (PCII) Program to prevent disclosure under the Freedom of Information Act (FOIA) and similar state and local disclosure laws. PCII also cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements.

CONTACT ICS-CERT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free:1-877-776-7585

For Control System Security Program Information and Incident Reporting:

http://www.us-cert.gov/control_systems/

DOCUMENT FAQ

What is an ICS-CERT Bulletin? An ICS-CERT Bulletin is intended to provide awareness or solicit feedback from US critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

Can I edit this document to include additional information? This document may not be edited or modified in any way by recipients, nor may any markings be removed. It may not be posted on public websites. All comments or questions related to this document should be directed to the ICS-CERT at ICS-CERT@dhs.gov.