Maintaining security in emergencies

An important part of the electric utility experience in North America is mutual assistance: Utilities that are besieged by storms, floods, fires and other disasters are aided by other utilities that aren't experiencing the same difficulties. The biggest component of this assistance is personnel who help with restoring lines, substations and other facilities that have been impacted by the disaster.

However, no utility wants to allow strangers to access its facilities without first verifying where they came from. This usually isn't very easy: Given the urgency of putting these people to work right away, often the only option is to scrutinize the ID card from the utility that employs the person, then hope it isn't just an elaborate forgery.

There's another problem with accepting guest workers: Often many, if not all, of the NERC CIP requirements for verification of personnel with access to BES Cyber Systems need to be set aside during the emergency. After all, nobody has time to do a seven-year background check on a worker from a neighboring utility who is needed immediately to replace relays in a flooded substation.

Of course, during the emergency your utility will usually declare CIP Exceptional Circumstances (CEC) to be in effect. However, CEC doesn't simply erase your obligation to verify that the people who showed up claiming to be employees of a neighboring utility were actually who they said they were; it simply postpones it. Wouldn't it be great if you could positively authenticate guest workers in the same way you can authenticate your own employees? You can!

XTec has years of experience helping authenticate guest workers in an emergency. We have worked with the Federal Emergency Management Agency (FEMA) when they have had to set up field offices to handle disasters like Superstorm Sandy, in which they typically need to authenticate hundreds or even thousands of workers.

If your organization has deployed XTec, you have access to tools that allow you to rapidly enroll and authenticate both your own employees and those that come to assist you from other utilities in the field – in four ways.

First, XTec can set up mobile enrollment and authentication facilities and staff them as needed. Someone from a different utility (or a contractor employee) just needs to bring two forms of government identification. Once the guest worker has been enrolled, they can be authenticated via a mobile card reader and get to work immediately. Of course, your own employees will only need to be authenticated, since they would already be enrolled.

Second, XTec's cards are based on the PIV standard used by the federal government. PIV cards are based on open standards and are interoperable across organizations. If any guest workers come from an organization that already uses PIV or CAC cards for authentication (whether or not they're XTec's cards), you can import those users into AuthentX, XTec's Identity Management System. When you have done that, you will be able to authenticate those "foreign" cards and automatically enroll the guest workers in AuthentX. With the access controls in AuthentX, you can then give them authorization to areas and networks you deem necessary, such as substations or warehouses. Finally, you can authenticate the guest workers, so they can get to work.

Third, before leaving for the site, your employees – as well as employees of other XTec customers that are providing assistance – can install a “derived credential” on their smart phone. This can be used in place of their PIV card to download protected documents, access applications and enter permitted facilities with mobile devices.

Finally, once the emergency is over and your utility has declared an end to the CIP Exceptional Circumstances, you will have documentation of exactly who had access to which facility at what time. Even more importantly, you will be able to confirm with the utilities who provided workers that they followed best practices when they onboarded the employees who came to help your utility. This includes conducting the Personnel Risk Assessment required by CIP-004-6 R3, if applicable. You will be able to provide this as evidence to the auditors that you didn’t take any unnecessary risks in admitting workers to your facilities, even during the emergency.