BOMGAR™

SECURE ACCESS AND NERC CIP VERSION 6 CYBER SECURITY STANDARDS

NERC CIP v6 REQUIREMENT FOR REMOTE ACCESS

In 2007, the Federal Energy Regulatory Commission (FERC) commissioned the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) as a mandatory standard within the United States. In 2016, FERC approved version 6 of the CIP standard. CIP V6 builds upon previous versions, particularly in the areas of security awareness, physical security, remote access and incident response.

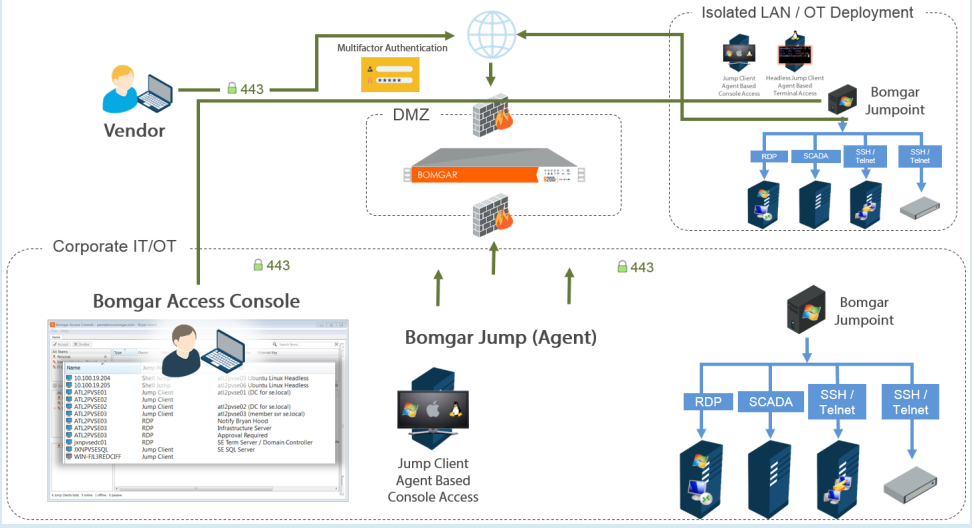
Many of these organizations have already realized that the VPNs or similar technologies they are using for remote access do not meet the standards set forth in CIP V6. When a VPN connection is used for remote access it gives the external vendor or remote user direct access to the Bulk Electric System (BES) cyber systems. This violates the controls set forth in these two sections of CIP V6. In addition, it is difficult to meet other auditing and reporting mandates within the mandate using a legacy VPN system.

Bomgar's Secure Access solution enable organizations to control, monitor, and audit access by privileged users and third-party vendors. Both the remote user and the endpoint connect to the Bomgar appliance via outbound connections, eliminating the need for a VPN tunnel that provides a direct connection. And users can use protocol tunneling to extend remote connectivity and auditing capabilities of proprietary and third-party applications without disrupting existing infrastructure.

In addition, Bomgar allows organizations to granularly set session permissions and record and monitor session activity, supporting CIP V6 standards outlined on the Electronic Security Perimeters Table R1. Using Bomgar, security administrators can see and approve when a third-party or vendor needs access to their internal systems, limit which systems or applications they can see and access, and monitor all activity from their desktop or mobile device.

Finally, Bomgar helps organizations to meet CIP requirement 2.3, which calls for multi-factor authentication for all interactive remote access sessions. Authentication is a major challenge throughout the energy sector where old machine accounts and shared accounts are often widespread. Through Bomgar's identity management solution, energy organizations can meet this requirement while improving their level of threat protection.

Bomgar in a NERC Environment



Bomgar and NERC CIP: A Perfect Fit

Bomgar solutions enables organizations to address NERC CIP security and compliance requirements while contributing to a true defense-in-depth strategy. With a cost-effective licensing model and a secure, robust, architecture capable of supporting up to tens of thousands of critical systems, Bomgar is the ideal choice for large, geographically dispersed environments. Bomgar enables you to:

- **IMPROVE** cybersecurity by closing the door on the #1 attack pathway for hackers, remote access
- **REPLACE** multiple legacy remote access tools with a single, comprehensive solution
- **INCREASE** productivity and security by eliminating the use of password spreadsheets and sticky notes for storing credentials
- **STANDARDIZE** the authentication process by enabling MFA, integrating with Smart Cards and identity management systems
- **SECURE** access across hybrid environments to support diverse IT infrastructure components
- **SIMPLIFY** regulatory compliance
- **IMPLEMENT** a solution your users will love

Meeting NERC CIP Compliance

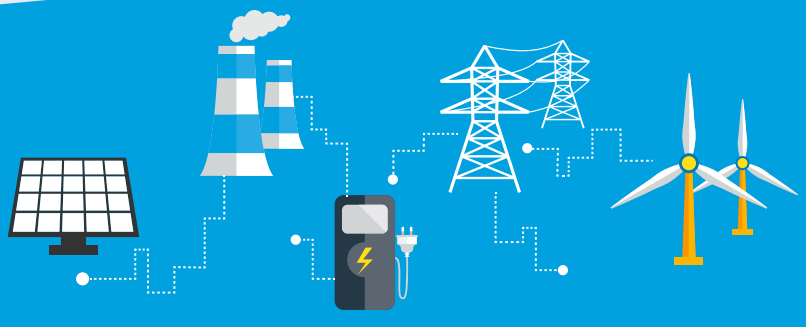
The standard requirements are represented in two main sections covering "Electronic Security Perimeter" and "Interactive Remote Access Management". Bomgar Privileged Identity and Access Management solutions can help organizations to meet these requirements and satisfy CIP V6 mandates.

ELECTRONIC SECURITY PERIMETER (ESP) TABLE R1

REQUIREMENT	BOMGAR RESPONSE
R 1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Bomgar is an on-premises appliance which can reside within the ESP. The appliance facilitates secure access to cyber assets and secures routable protocols through layered granular access controls; giving administrators a detailed view of session activity around cyber assets.
R 1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Bomgar enables secure access to assets within the EAP. All connections are outbound through the centralized Bomgar appliance and can be monitored and terminated by administrators, allowing Bomgar to act as an EAP for external connectivity.
R 1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	Bomgar allows organizations to implement granular access controls and set up approval workflows that trigger real-time approval requests, notifications, and require approvers to input reason for granting access.
R 1.4 Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	With Bomgar, authentication is required for access. Only the appliance facilitates access, allowing secure connectivity to cyber assets.
R 1.5 Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	Bomgar's recording features provide live surveillance and monitoring capabilities. All activity, whether malicious or non-malicious, is recorded and can be automatically populated into your SIEM tool. Malicious activity can not only be detected by the SIEM tool, but auditors can look back and see exactly what happened through video logs of all access activity.

INTERACTIVE REMOTE ACCESS MANAGEMENT TABLE R2

REQUIREMENT	BOMGAR RESPONSE
R 2.1 Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Bomgar governs access to nearly any system or device, anywhere, while keeping sensitive data and system access behind your own secure firewall. Unlike legacy solutions, such as VPN, there is no direct or unmonitored access to cyber assets since all access is brokered through the secure appliance.
R 2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	All Bomgar access sessions utilize the latest TLSv1.2 encryption technologies that are terminated at the appliance.
R 2.3 Require multi-factor authentication for all Interactive Remote Access sessions.	Bomgar Secure Access solutions include native MFA that can easily be enabled for all users, at no additional cost.



Make Least Privilege Productive – Quickly

Bomgar helps security and IT support professionals be compliant with NERC CIP regulations and improve business performance by enabling secure, controlled access to nearly any device or system, anywhere in the world.

REMOTE SUPPORT

Super-fast, all-inclusive remote support for IT service desks and customer tech support

PRIVILEGED ACCESS

Manage and monitor privileged access to critical systems... without VPN

PRIVILEGED IDENTITY

Continuous, automated account discovery protects privileged credentials at scale

PROTECT THE OPERATIONAL TECHNOLOGY AT THE HEART OF YOUR BUSINESS

Bomgar Secure Access Solutions enables power and energy plants to securely manage their networks and operate within compliance of strict cyber security regulations set by NERC. Bomgar quickly protects your critical production technology and can help your organization to strengthen security, minimize operational downtime, and increase productivity.

To learn more about Bomgar's secure access solutions visit: **www.bomgar.com**

ABOUT BOMGAR

Bomgar is the leader in Secure Access solutions that empower businesses. Bomgar's leading remote support, privileged access management, and identity management solutions help support and security professionals improve productivity and security by enabling secure, controlled connections to any system or device, anywhere in the world. More than 13,000 organizations across 80 countries use Bomgar to deliver superior support services and reduce threats to valuable data and systems. Bomgar is privately held with offices in Atlanta, Jackson, Washington D.C., Frankfurt, London, Paris, and Singapore. Connect with Bomgar at www.bomgar.com.

CONTACT | **INFO@BOMGAR.COM** | **866-205-3650 (U.S.)** | **+44 (0)1628-480-210 (U.K./EMEA)** | **BOMGAR.COM**