NORTHERN PLAINS AREA
Policy Memorandum

DATE:	March 14, 2008
SUBJECT:	Building Automation and Control Systems (BAS or BCS)
NUMBER:	PM-05-006
EFFECTIVE DATE:	Immediately Until Replaced or Superseded (Replaces PM-05-006 dated August 18, 2005)

1. Background

Most building automation and control systems (BAS or BCS) today are typically managed remotely by means of dial-up modem and are isolated from Agricultural Research Service (ARS) Local Area Networks (LAN's). However, the building automation industry is migrating from isolating BAS or BCS toward integrating them into a shared LAN. These systems monitor heating, ventilation, and air conditioning (HVAC), security, and even fire alarms most of which are being controlled by workstation computers and allow remote monitoring capability. Some workstations**,** installed by outside vendors**,** may also be configured with Internet Information Services (IIS) web services enabled, which then is accessible via an Internet browser using both secured and unsecured protocols. If it is secured, access includes use of a virtual private network (VPN) or key and certificates. If it is not secured these workstations are generally open to the Internet. These workstations are sometimes not managed or patched and can potentially be compromised from outside sources.

2. Purpose

In an effort to leverage IT security best practices, the Northern Plains Area (NPA) has instituted a policy to minimize BAS or BCS vulnerabilities and security breaches on its local and wide area networks.

3. Threats

LAN-based BAS or BCS have resources that make them as attractive to hackers as a normal desktop personal computer (PC). Potential threats when the BAS or BCS installed on the shared IT network include:

Hackers, both mischievous and malicious, perform criminal activities, which include denial of service (DoS) attacks, theft, and destruction of property.

Disgruntled employees may act as hackers using knowledge of the networks, computers, and protocols to perform unauthorized actions.

Criminal activities include gathering information that would give knowledge of the buildings and how to break in, or even getting into the security system and having doors open.

Competitors could monitor the network and gather information regarding utility uses such as electricity or gas.

4. Policy

All LAN-based BAS or BCS accessible from the Internet, shall be firewalled, include anti-virus protection, maintain patch management reporting capabilities, and be either physically isolated off ARS-owned LAN's or logically through use of established Virtual Local Area Network (VLAN). Updates to anti-virus and patch management can be manual or automatic depending on the testing requirements of the BAS or BCS provider.

Any inbound or outbound port traffic will be limited at the firewall and will be based on the needs of the BAS or BCS provider. If remote access is needed, static Internet Protocol (IP) addresses can be assigned. Outside access however, must be limited to either a specific IP address or at most a Class C IP address subnet assignment. Use of a VPN client application is also permitted.

Further, if the responsible Accrediting Official determines that the BAS or BCS lack of security protection poses a threat to the network, the Accrediting Official reserves the right to require that access to the BAS or BCS be through a dedicated digital subscriber line (DSL) or dialup service.

5. Implementation

The Cisco PIX hardware appliance firewall is the NPA standard. It has been deployed and has proven to be a sound solution for locations throughout the NPA in protecting ARS-owned local and wide area networks. Deployment of this solution allows for the physical isolation of the BAS or BCS on a segmented portion of the network by installing a second Ethernet module in the PIX. Inevitably, this would result in having the BAS or BCS on its own LAN. It is recommended that the port be setup with network address translation (NAT) using an established private IP space to further protect the BAS or BCS from being compromised.

In cases where physical isolation is not possible, VLAN's shall be utilized to logically isolate these devices. It is noted that use of VLAN's may require replacement of network switching devices, which support layer 3.

6. References

1. Holmberg, D.G. 2003. “BACnet wide area network security threat assessment.” National Institute of Standards and Technology (NIST) Internal Report 7009. http://fire.nist.gov/bfrlpubs/build03/PDF/b03034.pdf

2. Holmberg, D.G. 2003. “Enemies at the gates.” member of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Supplement Journal. http://fire.nist.gov/bfrlpubs/build03/PDF/b03083.pdf

7. Point of Contact

For further information, please contact the Area Information Technology Office.

/s/
W.H. BLACKBURN
Area Director
Northern Plains Area