

July 23, 2013

INFORMATIONAL ITEM

MEMORANDUM TO THE TRUSTEES

FROM THE CHIEF INFORMATION SECURITY OFFICER

SUBJECT: Authority Cyber Security Overview

SUMMARY

This memorandum provides an informational item to the Trustees on the Authority's cyber security activities.

BACKGROUND

At the request of the President and Chief Executive Officer, the Chief Information Security Officer is providing this update on the Authority's cyber security activities.

DISCUSSION

The PowerPoint presentation (Exhibit "A") represents an informational update on the cyber security activities.



New York Power Authority

Generating more than electricity

Cyber Security Overview

Lena Smart
Chief Information Security Officer

July 23rd, 2013
Board of Trustees Meeting

Cyber Security Overview

NYPA IT Cyber Security Group created 10 years ago

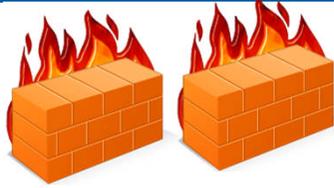
- Staffed by qualified cyber security subject matter experts
- Expertise in computer forensics, data recovery, data security, network security
- NYPA staff and contractors are given mandatory annual cyber awareness training
- Cyber Security Team publishes monthly security bulletins for all staff
- We work closely with the NY State cyber security staff
- I am the Energy Sector Chief for the FBI Infragard – a collaboration between public and private sectors and my staff are all members of FBI Infragard
- We practice layered security

Layered Security



The Internet

*D
M
Z*



Firewalls



Secure remote access



Internet filters

*Security
Operations
Center
Monitoring*



*Internal
Network & Desktop
Monitoring*

*I
N
T
E
R
N
A
L*



*Cyber
Awareness
Training*



*Server &
Desktop
Firewalls*



*Server &
Desktop
Lockdown
Policies*



*Anti Virus
Software*

Tools to help

- Firewalls – we can block entire countries from knowing that we exist
- Security Operations Center – they monitor our critical assets 24x7x365 and alert us to anomalies
- Intrusion Prevention Devices – stops viruses or malware at a specific site and doesn't allow it to infect the rest of NYPA network
- Anti virus software runs on all servers and desktops, constantly checking for malware
- We perform our own penetration tests and vulnerability assessments, and also engage 3rd parties to try and “hack us”
- Recently installed hardware and software to mitigate against Distributed Denial of Service attacks
- Working with National Labs on desktop security solutions