



# Maturing Cybersecurity at CFISD

On **Monday, June 18, 2018** CFISD employees met with **George Reeves**, a Cybersecurity Advisor for the Dept. of Homeland Security. (DHS) The DHS offers a number of programs and services to help K-12 communities build, sustain, and promote resiliency to the threats that confront institutions across the nation. Among services and programs that we are looking into implementing include but are not limited to the following:

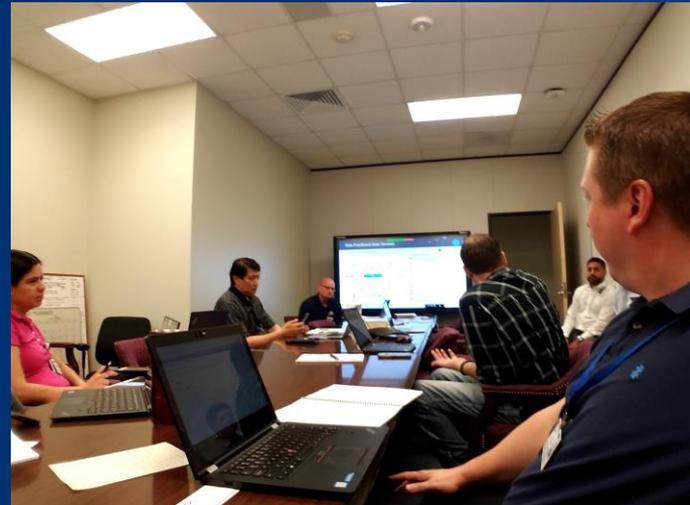


- Tabletop exercises to walk through hurricane and data breach response
- Cyber Assessments to identify and reduce areas of risk, including external dependency management to reduce risk from third parties.
- Cyber Hygiene vulnerability scanning
- Validated Architecture Design Review for an in depth look into our network architecture design and interconnectivity, focused on defensive strategies.

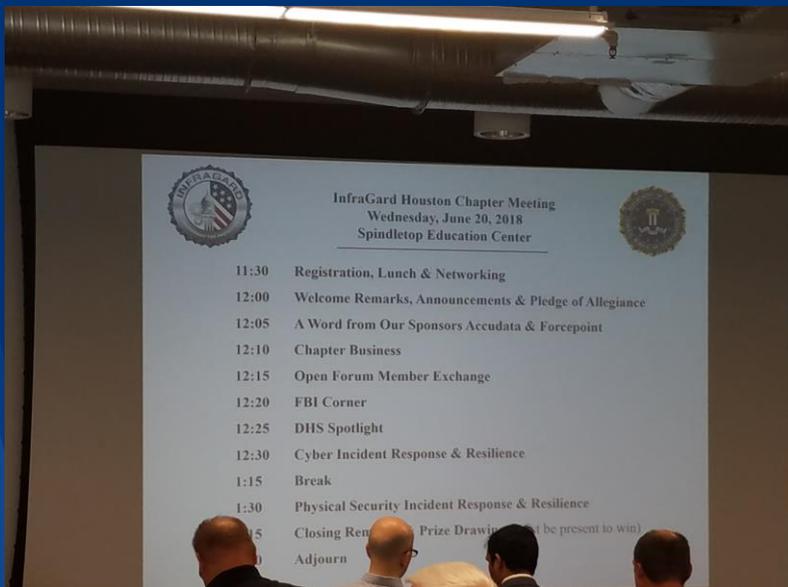


# Network Visibility and Security

On **Tuesday, June 19, 2018**, ForeScout provided a hands on lab to demonstrate how their product can be used to provide visibility to all devices on our network, and how to create rules to ensure better network control. In attendance from CFISD were **Andrew Tran, Elizabeth Montez, Oscar Villar, David Deitsch, and James Costello**.



On **Wednesday, June 20<sup>th</sup>, 2018**, **James Costello** was able to attend the monthly InfraGard meeting. InfraGard is the collaboration of the FBI working with the local agencies and companies in order to better protect ourselves from cyber attacks. See more information about the InfraGard meeting below.





# June InfraGard Meeting

The main topic of this month's InfraGard meeting was incident response, and how to best prepare for inevitable cyber attacks or natural disasters. The steps that were detailed included:

**Prepare** – Keep a detailed plan in a hard and soft copy. Include detailed procedures for each IR stage. Assemble the right people, based on skill diversification, quality, and team size, and ensure those team members are trained. Perform tabletop exercises regularly to ensure that the necessary actions are memorized and able to be performed without too many additional questions.

**Identification** – Identify what happened, who was affected, what technology was affected, and how it happened.

**Containment** – Keep the problem from getting worse. Pull necessary systems off the network, change passwords, etc.

**Eradication** – Eradicate the issue by restoring from most recent backup. Implement new protection techniques, apply new firewall rules, apply patches, etc.

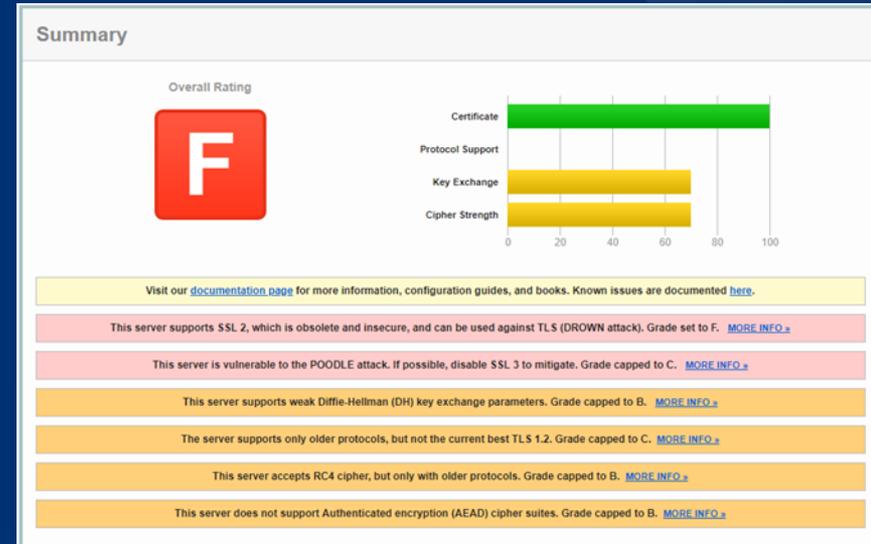
**Recovery** – Put systems back into production in a safe manner. Validate and monitor the systems.

**After Action Review** – What can be implemented to find and stop the issue more quickly next time. The goal is for continued improvement in preventing or responding to security issues.



# Qualys SSL Server Test Results

Qualys SSL server test is part of the district's vetting process to ensure vendor web servers have proper SSL configurations. Rank One Sport ([www.rankonesport.com](http://www.rankonesport.com)) was contacted regarding their "F" rating which pointed to critical vulnerabilities in their web server configuration. Rank One Sport worked with their programmers and corrected the vulnerabilities, going from an F to an A rating. They appreciated the notice and were happy to work together to ensure proper standards are being followed, all in an effort to safeguard sensitive student information.



First Rating

## Qualys SSL Server Test

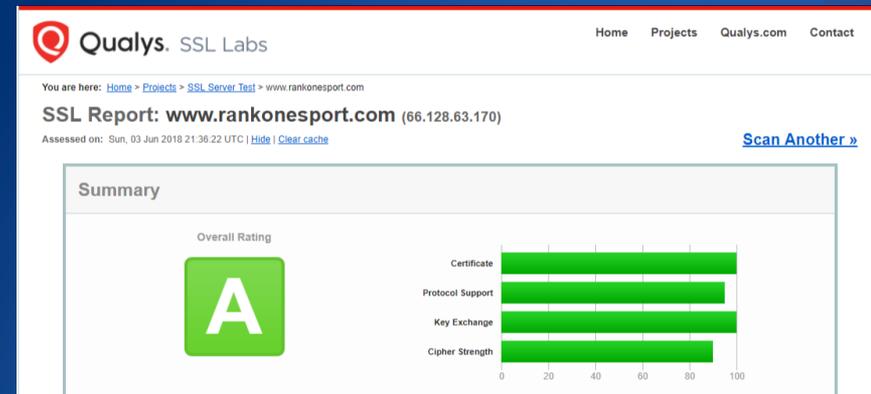
<https://www.ssllabs.com/ssltest/index.html>



The SSL server test is an online service that enables you to inspect the configuration of any public SSL web server.

This free service is a helpful tool to verify basic SSL security protocols are in place on websites that may be handling student data.

Users enter the desired web address to begin the analysis of that site's SSL configuration. A SSL Server rating will be displayed at the completion of the analysis.



Second Rating