# Cyber Hygiene™ (CH)

- Overview
  - Cyber Hygiene™ activities focus on increasing the general health and wellness of the cyber perimeter by broadly **assessing NCCIC stakeholders internet accessible systems for known vulnerabilities and configuration errors** on a **recurring** basis. As potential issues are identified the NCATS team will work with impacted stakeholders to **proactively mitigate threats and risks** to their systems prior to their exploitation by malicious third parties.
  - Stakeholder specific data is for stakeholder eyes only
- Objectives
  - Establish an enterprise view of the FCEB, SLTT, and critical infrastructure public cybersecurity posture
  - Understand how we appear to an attacker
- Benefits
  - **Complements** an existing security program and capabilities
  - Provides an **objective view** of current public security posture
  - **Reduced exposure** to known threats

# Cyber Hygiene™ Activities

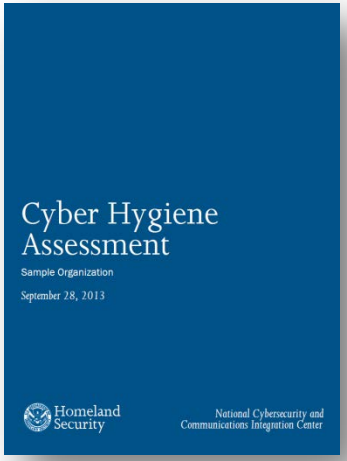
## Network Mapping

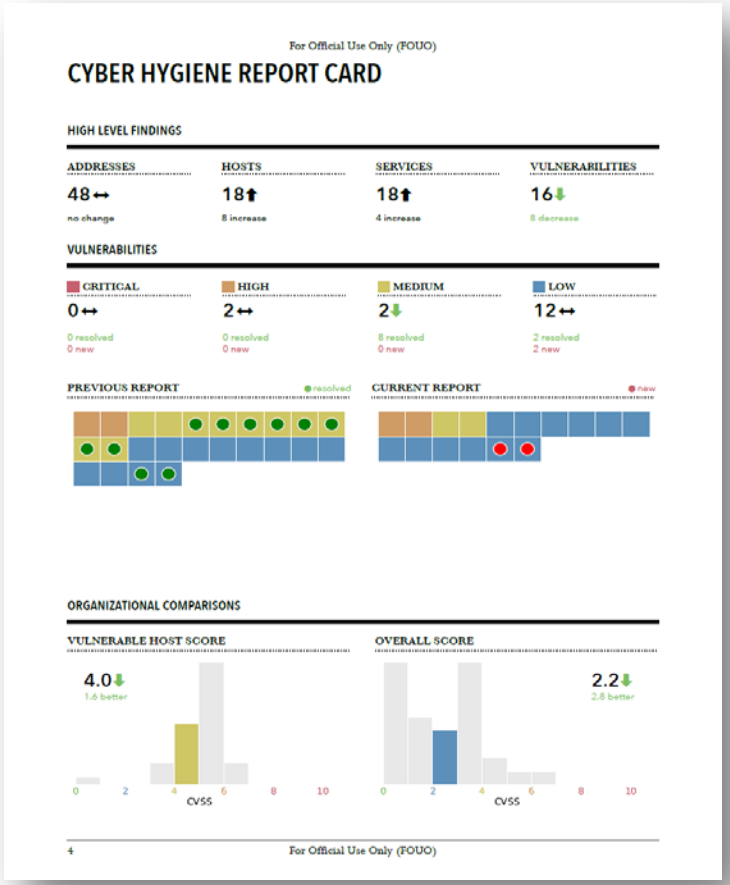
- Identify public IP address space
- Identify hosts that are active on IP address space
  - *Determine the O/S and Services running on the active hosts*
  - *Re-run scans to determine any changes on IP address space*
- Graphically represent address space/system on geographical map

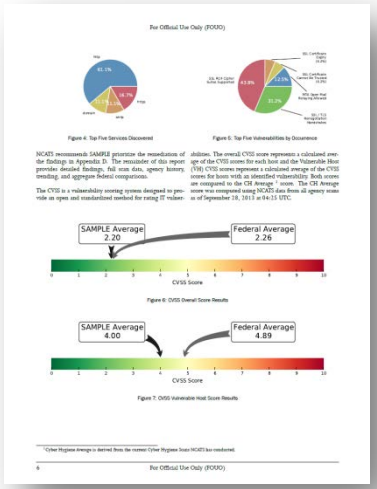
## Network Vulnerability & Configuration Scanning

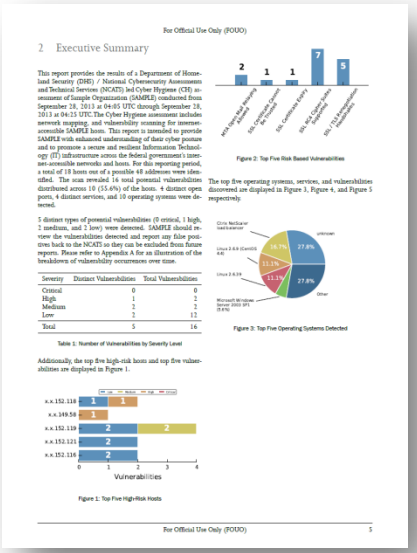
- Identify network vulnerabilities and weaknesses
- Identify common configuration errors in scanned assets such as
  - *Improperly signed Domains (DNSSEC)*

# CH™ Sample Report Snapshots



# Cyber Hygiene™ - FAQ

- **How frequently will the scans occur?**
  The frequency of the scans is up to you. In addition to on-demand scans, NCATS would like to conduct quarterly, monthly, or weekly scans.

- **Who schedules the scans?**
  Once we receive the signed authorization letter, we assign a Technical POC to work with your agency POC to validate /determine your public IP space and identify the frequency and time frames the scanning may occur.

- **Is "white listing" expected?**
  Your agency is not required or expected to "white list" the DHS scanning range, although the results will be more thorough if you do. The choice is entirely up to your agency. A couple of days prior to scanning activity we send notification letters (email) to US-CERT and to any identified agency SOCs explaining the activity and identifying the source IP range so they will be prepared.

- **What level of access is granted to the reports and data?**
  In addition to the report we prepare you will have full access to all data and findings produced by our tools

# Cyber Hygiene™ – FAQ, con't

- **What information is included in the report?**
  - A listing of systems detected, open ports, services/applications (with version number) and operating system running on those systems
  - A listing of known vulnerabilities (if any) specific to the applications running
  - A listing of vulnerabilities identified on each system
  - A summary / validation of your public 2nd level domain DNSSEC status (e.g. dhs.gov, tsa.gov)
  - For comparison statistics, non-attributable ***Totals & Averages*** for all previous data points will be provided
  - Reports will also provide trending/history and highlight any delta's between the current and previous report

- **What value will be provided**

  In addition to providing a free, 3rd party, objective perspective of the vulnerabilities present and risks to your internet connected assets, participation will benefit NCCIC stakeholders as a whole. A major objective is to provide a non-attributable but quantifiable data source to senior leadership to ensure initiatives and policy directives are well informed, fact based, and focused on areas with the greatest need.