



# Cyber Hygiene™ (CH)

- Overview

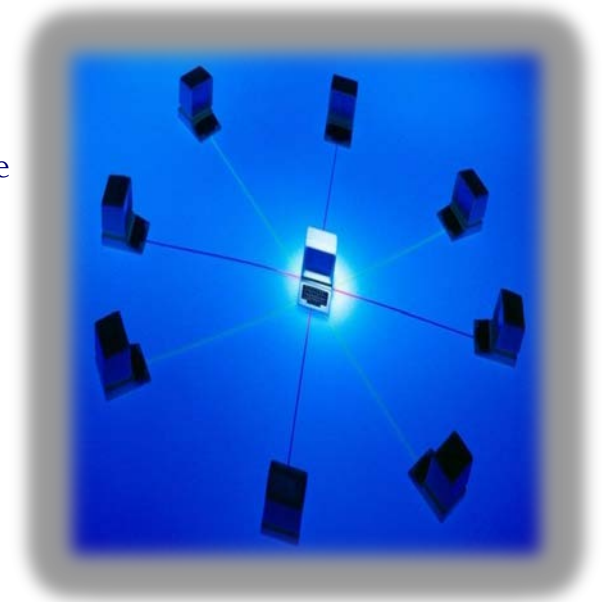
- Cyber Hygiene™ activities focus on increasing the general health and wellness of the cyber perimeter by broadly **assessing NCCIC stakeholders internet accessible systems for known vulnerabilities and configuration errors** on a **recurring** basis. As potential issues are identified the NCATS team 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 Snapshot

**Cyber Hygiene Assessment**  
 Sample Organization  
 September 28, 2013

Homeland Security  
 National Cybersecurity and Communications Integration Center

For Official Use Only (FOUO)

## CYBER HYGIENE REPORT CARD

**HIGH LEVEL FINDINGS**

ADDRESSES	HOSTS	SERVICES	VULNERABILITIES
48 ↔ no change	18 ↑ 8 increase	18 ↑ 4 increase	16 ↓ 8 decrease

**VULNERABILITIES**

CRITICAL	HIGH	MEDIUM	LOW
0 ↔ 0 resolved 0 new	2 ↔ 0 resolved 0 new	2 ↓ 8 resolved 0 new	12 ↔ 2 resolved 2 new

**PREVIOUS REPORT** ● resolved **CURRENT REPORT** ● new

**ORGANIZATIONAL COMPARISONS**

**VULNERABLE HOST SCORE**

4.0 ↓  
1.6 better

**OVERALL SCORE**

2.2 ↓  
2.8 better

For Official Use Only (FOUO)

For Official Use Only (FOUO)

## 2 Executive Summary

This report provides the results of a Department of Homeland Security (DHS) National Cybersecurity Assessment and Technical Services (NCATS) and Cyber Hygiene (CH) assessment of Sample Organization (SAMPLE), conducted from September 18, 2013 to 04:33 UTC through September 18, 2013 at 04:33 UTC. The Cyber Hygiene assessment includes network scanning and vulnerability scanning for Internet-accessible SAMPLE hosts. This report is intended to provide SAMPLE with enhanced understanding of their cyber posture and to promote a secure and resilient Information Technology (IT) infrastructure across the Federal government's Internet-accessible networks and hosts. For this reporting period, a total of 18 hosts out of a possible 48 addresses were identified. The scan revealed 24 total potential vulnerabilities distributed across 10 (55.6%) of the hosts. A distant open port, 4 distant services, and 10 operating systems were detected.

**Figure 2: Top Five Risk Based Vulnerabilities**

The top five operating systems, services, and vulnerabilities discovered are displayed in Figure 3, Figure 4, and Figure 5 respectively.

**Figure 3: Top Five Operating Systems Detected**

**Table 1: Number of Vulnerabilities by Severity Level**

Severity	Distant Vulnerabilities	Total Vulnerabilities
Critical	0	0
High	1	2
Medium	2	2
Low	2	11
Total	5	16

**Table 2: Top Five High-Risk Hosts**

For Official Use Only (FOUO)

For Official Use Only (FOUO)

**Figure 4: Top Five Services Discovered**

**Figure 5: Top Five Vulnerabilities by Occurrence**

NCATS measures the SAMPLE organization's readiness to detect and respond to threats. The results of this report provide detailed findings, full scan data, agency history, and aggregate threat intelligence. The CH score represents a calculated average of the CVSS scores for each host and the 'Vulnerable Host Score' (VHS) CVSS score represents a calculated average of the CVSS scores for each host as identified vulnerabilities. Both scores are reported to the CH Average Score. The CH Average Score was calculated using CVSS data from 48 agencies across all of September 18, 2013 at 04:33 UTC.

**Figure 6: CVSS Overall Score Results**

**Figure 7: CVSS Vulnerable Host Score Results**

For Official Use Only (FOUO)



# 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, 3<sup>rd</sup> 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.