

16 Oct 2012



Homeland
Security

Homeland Security Perspectives: Cyber Security Partnerships and Measurement Activities

Bradford Willke

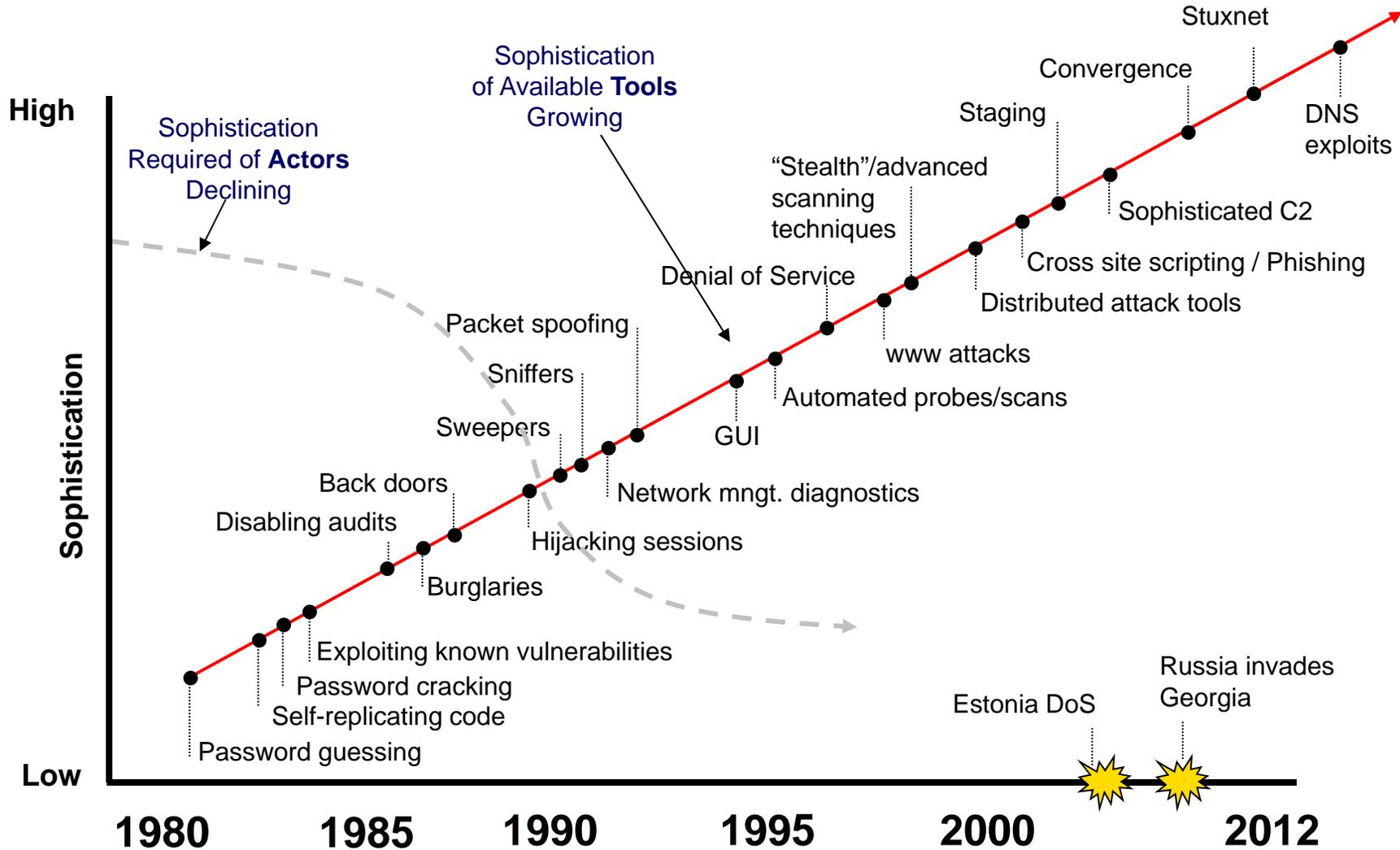
Cyber Security Advisor, Mid-Atlantic Region

National Cyber Security Division (NCSD)

Office of Cybersecurity and Communications (CS&C)

U.S. Department of Homeland Security (DHS)

Growth of Cyber Threats



Homeland Security

Unclassified // For Unlimited Distribution

Cyber Partnership Examples

- ▶ AMSC Cyber Sub-Committee (Pittsburgh)
- ▶ MS-ISAC (Multi-State Information Sharing and Analysis Center)
- ▶ Ohio Statewide Cyber Security Strategy
- ▶ VALGITE (Virginia Local Government IT Executives)
- ▶ VOICCE (Virginia's Operational Integration Cyber Center of Excellence)



Area Maritime Security Committee: Cyber Sub-Committee

- ▶ DHS, USCG, CIKR, and Business Partnership
- ▶ Committee Premises:
 - Incident response and continuity of operations *still* need work
 - Partners need credible planning templates and test-able scenarios
 - A SME database for cyber responders is useful and needed
 - Organizations need a “411” system for information on where to voluntarily report, request technical assistance, request non-technical incident handling, request law enforcement responses, to cyber incidents
 - Organizations would benefit from a local emergency management, “911-like,” function that mobilizes regional and local cyber responses – and creates a regional common operating picture



MS-ISAC Overview

- ▶ State, Local, Territorial, and Tribal Partnership
- ▶ Operated by NY-based Center for Internet Security
- ▶ Operational Services:
 - Incident coordination, handling, and response
 - “Albert” services for threat monitoring, detection, and prevention
 - Fee-for-Service model for vulnerability and “PEN” testing
 - Low cost (\$.75/student) for annual cyber security awareness & training
 - **FREE** post-incident vulnerability and mitigation service
 - Broad assistance with state and local incidents, much beyond *cyber*



Ohio Statewide Cyber Strategy

- ▶ Developed in 2011; adopted in 2012
- ▶ Led by Ohio Homeland Security Advisory Council – Cyber Working Group
 - Direct ties to Ohio Strategic Analysis and Information Center (SAIC)
 - Co-chaired by Ohio Chief Information Security Officer and Ohio Office of Homeland Security
- ▶ Organizes both internal, state-focused and external, partner –focused (i.e., academia, private sector, public sector) activities
- ▶ Creates a twelve-month, renewable action plan, with five initiatives:
 - Initiative 1: Share cyber security threat information across the homeland security enterprise
 - Initiative 2: Create a cyber security culture in state and local government
 - Initiative 3: Partner with the public and private sectors to support their cyber security efforts
 - Initiative 4: Identify cyber resources (human and equipment) to leverage for creating cyber incident response teams
 - Initiative 5: Raise cyber security awareness across Ohio



**Homeland
Security**

NATIONWIDE CYBER SECURITY REVIEW (NCSR)



**Homeland
Security**

NCSR Methodology

- ▶ The NCSR methodology leveraged an existing cyber security controls framework developed by the MS-ISAC
 - The 2011 NCSR utilized a Control Maturity Model (CMM) to measure how effective the State and Local governments' risk management programs are at deploying a given cyber security control based on risk management processes
 - This methodology uses key milestones and benchmarks for measuring the effectiveness of security control placement based on risk management processes



NCSR Maturity Model

Level	Control Maturity Level Description
Ad-Hoc	<p>Activities for this control are one or more of the following:</p> <ul style="list-style-type: none"> - Not performed - Performed but undocumented / unstructured - Performed and documented, but not approved by management
Documented Policy	<p>The control is documented in a policy that has been approved by management and is communicated to all relevant parties.</p>
Documented Standards / Procedures	<p>The control meets the requirements for Documented Policy and satisfies all of the following:</p> <ul style="list-style-type: none"> - A full suite of documented standards and procedures that help guide implementation and management of the enterprise-wide policy - Communicated to all relevant parties
Risk Measured	<p>The control meets the requirements for Documented Standards / Procedures and satisfies all of the following:</p> <ul style="list-style-type: none"> - Control is at least partially assessed to determine risk - Management is aware of the risks
Risk Treated	<p>The control meets the requirements for Risk Measured and satisfies all of the following:</p> <ul style="list-style-type: none"> - A risk assessment has been conducted - Management makes formal risk-based decisions based on the results of the risk assessment to determine the need for the control - The control is deployed in those areas where justified by risk, but is not deployed where not justified by risk
Risk Validated	<p>The control meets the requirements for Risk Treated and satisfies all of the following:</p> <ul style="list-style-type: none"> - If the control is deployed (in those areas where justified by risk), the effectiveness of the control has been externally audited/tested to validate that the control operates as intended - If the control is not deployed (in those areas where not justified by risk), management's decision to not implement the control was determined to be sound



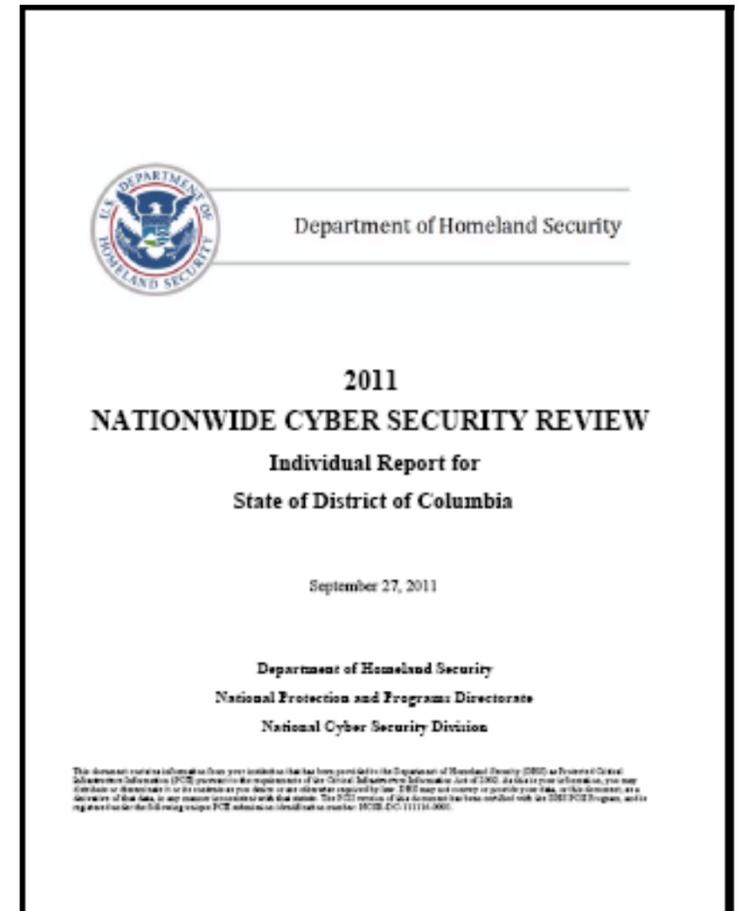
Methodology: Assessed Control Areas

- The 2011 NCSR examined 12 cyber security control areas:
 - Security Program
 - Risk Management
 - Physical Access Controls
 - Logical Access Controls
 - Security Within Technology Lifecycles
 - Information Disposition
 - Malicious Code
 - Monitoring and Audit Trails
 - Incident Management
 - Business Continuity
 - Security Testing



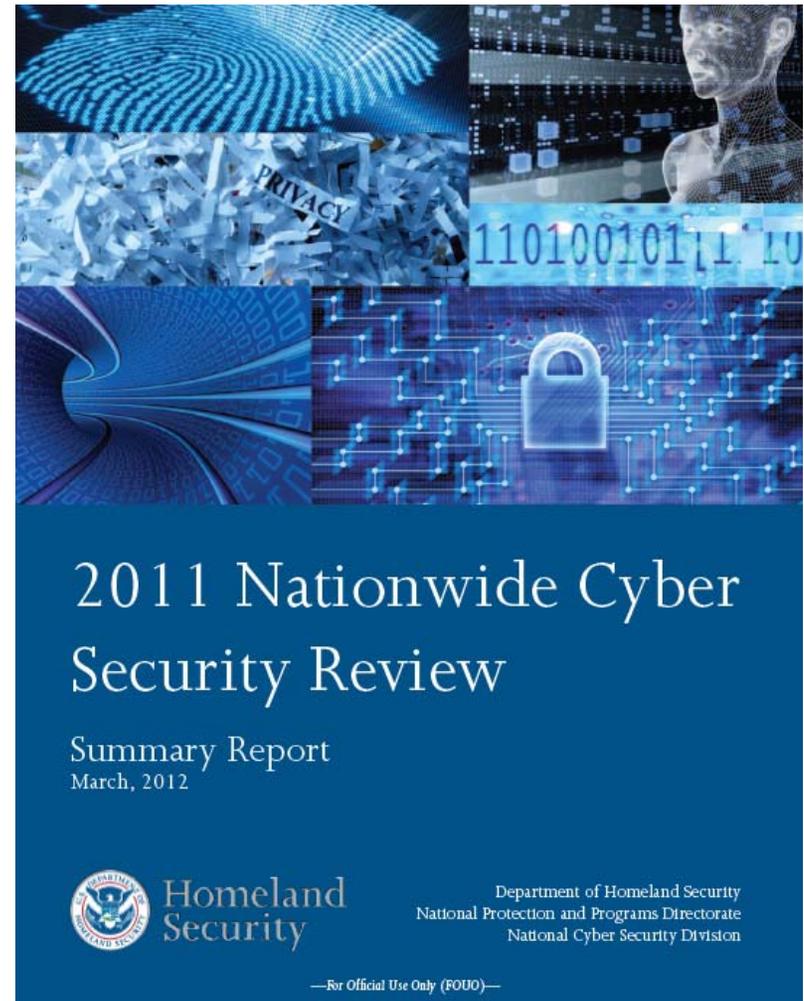
Individual Report

- ▶ Every respondent received a report immediately after they completed the review.
- ▶ The Individual Report included:
 - Details on the Reporting methodology;
 - A full list of the questions asked;
 - How the respondent answered each question, and;
 - High level options for consideration based on answers.
- ▶ The Individual Report was protected as PCII, and was only disseminated via the Secure US-CERT Portal.



Summary Report

- ▶ The NCSR Summary Report was released to respondents on March 16, 2012.
- ▶ The Summary Report highlighted key findings from the 2011 Review including identifiable gaps and recommendations on how States and Local governments can increase their risk awareness.
- ▶ The Summary Report will not be attributable to specific respondents or organizations.
- ▶ The Summary Report will allow respondents to compare their answers against the national averages and determine their individual strengths & weaknesses.



Comparison of Results

Appendix A: Participant Response Matrix

#	Question	All Submissions						States						State agencies						Local Governments					
		AH	DP	DSP	RM	RT	RV	AH	DP	DSP	RM	RT	RV	AH	DP	DSP	RM	RT	RV	AH	DP	DSP	RM	RT	RV
Security Program																									
1	Does your organization maintain an information security program that guides information security management, reporting, and controls?	18	22	30	15	6	10	5	20	34	20	9	11	14	22	29	17	5	12	32	22	28	8	3	7
3	Does your organization have roles and responsibilities (such as a Chief Information Security Officer or Information Systems Security Officer) for the management of your information security program?	30	18	23	9	7	13	11	23	30	11	7	18	21	21	28	10	5	16	52	12	15	7	8	7
4	Does your organization have reporting processes to periodically (at least annually) inform information security management on the effectiveness of the information security program?	42	14	14	15	7	9	25	18	23	18	7	9	34	14	16	17	7	12	62	10	7	10	7	5
Risk Management																									
5	Does your organization perform a thorough inventory and security categorization of its information and information technology assets (such as applications, databases, operating systems, networking devices, networking zones, etc.) that results in a formal information, risk, or security classification program?	47	14	15	19	3	1	32	20	16	23	5	5	38	14	22	24	2	0	67	10	8	12	3	0

Unclassified // For Unlimited Distribution

Results: Security Control Areas

Rank	Process Area	Ad-Hoc	Documented Policy - Documented Standards and Procedures	Risk Measured -Risk Validated
1	Malicious Code	12%	36%	52%
2	Physical Access Control	16%	39%	46%
3	Logical Access Control	18%	40%	42%
4	Security Testing	42%	22%	36%
5	Incident Management	32%	38%	31%
6	Business Continuity	33%	36%	31%
7	Personnel and Contracts	29%	41%	30%
8	Security Program	30%	40%	30%
9	Information Disposition	27%	44%	29%
10	Security within Technology Lifecycle	36%	35%	29%
11	Risk Management	45%	26%	29%
12	Monitoring and Audit Trails	46%	27%	28%



Key Findings: Capabilities and Gaps

Strengths:

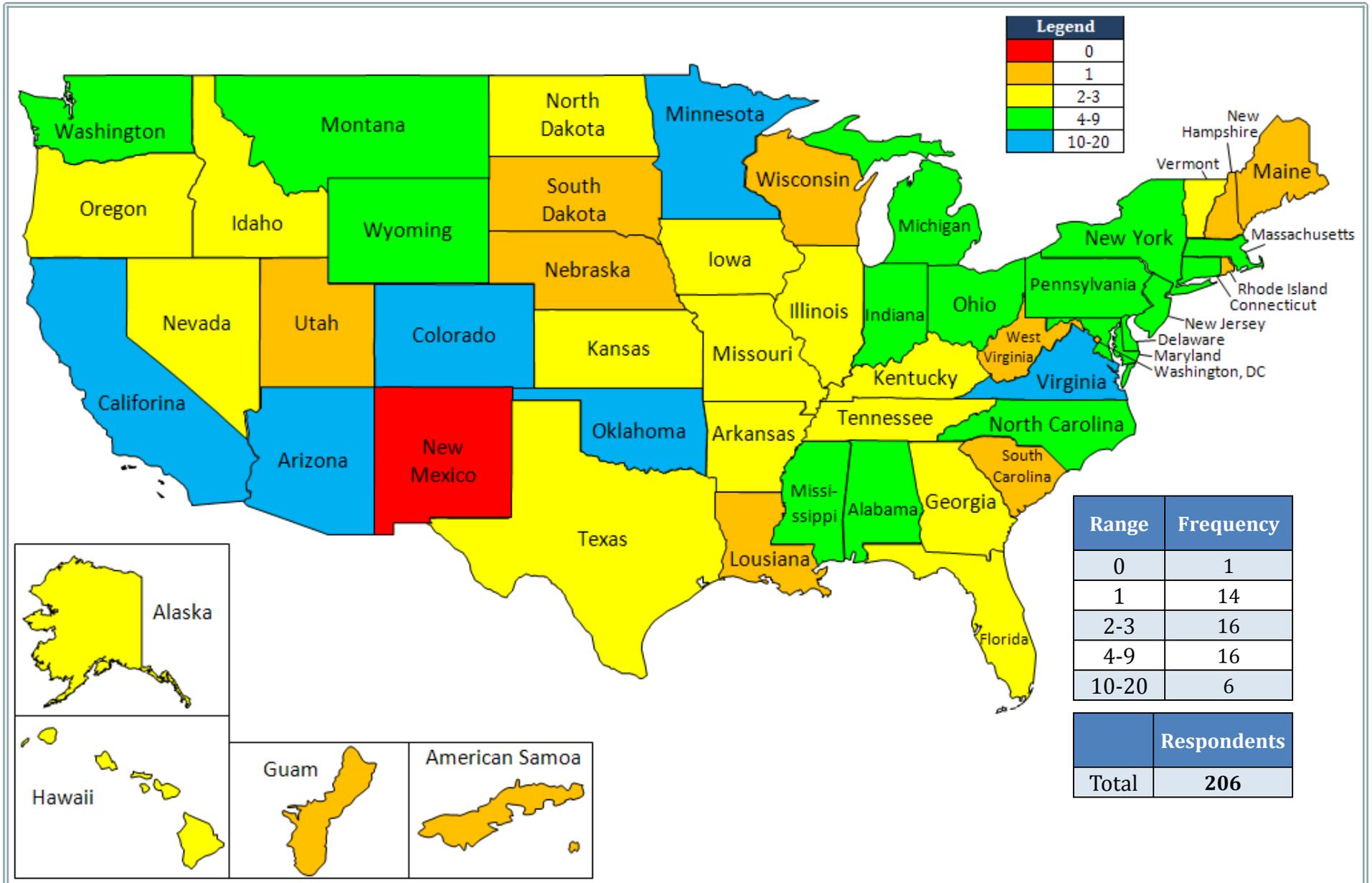
- 52% have implemented and/or validated protective measures for the detection and removal of malicious code
- 81% of all respondents have adopted cyber security control frameworks and/or security methodologies
- 42% have implemented and/or validated logical access controls (e.g., termination/transfer procedures, ACLs, remote access)

Weaknesses:

- 42% of respondents stated they do not have independent testing and/or audit program established
- 45% of respondents stated they have not implemented a formal risk management program (e.g., risk assessments, security categorization)
- 46% of respondents stated they have not implemented Monitoring and Audit Trails which is important to determine if an incident is occurring or has occurred.
- 31% of all respondents have never performed a contingency exercise
- 67% of all respondents stated it has been at least two years since they updated their Information Security Plan
- 66% of all respondents stated it has been at least two years since they updated their Disaster Recovery Plans



2011 Nationwide Cyber Security Review - Registered Respondents



ADDITIONAL DHS-LED CYBER SECURITY REVIEWS



**Homeland
Security**

Key Resilience Domains

AM	Asset Management <i>identify, document, and manage assets during their life cycle</i>	IM	Incident Management <i>identify and analyze IT events, detect cyber security incidents, and determine an organizational response</i>
CCM	Configuration and Change Management <i>ensure the integrity of IT systems and networks</i>	SCM	Service Continuity Management <i>ensure the continuity of essential IT operations if a disruption occurs</i>
RISK	Risk Management <i>identify, analyze, and mitigate risks to critical service and IT assets</i>	EXD	External Dependencies Management <i>establish processes to manage an appropriate level of IT, security, contractual, and organizational controls that are dependent on the actions of external entities</i>
CNTL	Controls Management <i>identify, analyze, and manage IT and security controls</i>	TRNG	Training and Awareness <i>promote awareness and develop skills and knowledge of people</i>
VM	Vulnerability Management <i>identify, analyze, and manage vulnerabilities</i>	SA	Situational Awareness <i>actively discover and analyze information related to immediate operational stability and security</i>



Maturity Not Just Capability

- A MIL (Maturity Indicator Level) measures *process institutionalization*, and describes attributes indicative of mature capabilities.

MIL Level 5 – Defined

All practices are performed (MIL-1); planned (MIL-2); managed (MIL-3); measured (MIL-4); and consistent across all internal constituencies who have a vested interest— processes/practices are defined by the organization and tailored by organizational units for their use, and supported by improvement information shared amongst organizational units.

MIL Level 4 – Measured

All practices are performed (MIL-1); planned (MIL-2); managed (MIL-3); and periodically evaluated for effectiveness, monitored & controlled, evaluated against its practice description & plan, and reviewed with higher-level management.

MIL Level 3 – Managed

All practices are performed (MIL-1); planned (MIL-2); and governed by the organization, appropriately staffed/funded, assigned to staff who are responsible/accountable & adequately trained, produces expected work products, placed under appropriate configuration control, and managed for risk.

MIL Level 2 – Planned

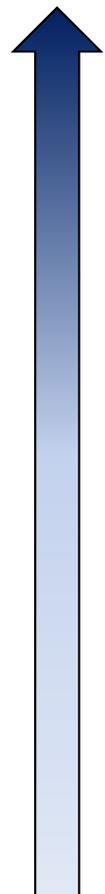
All practices are performed (MIL-1); and established, planned, supported by stakeholders, standards and guidelines.

MIL Level 1 – Performed

All practices are performed, and there is sufficient and substantial support for the existence of the practices.

MIL Level 0 – Incomplete

Practices are not being performed, or incompletely performed.





Homeland Security

Contact Information

Bradford Wilke

bradford.wilke@hq.dhs.gov

Department of Homeland Security
National Protection and Programs Directorate
Cyber Security and Communications



Homeland Security