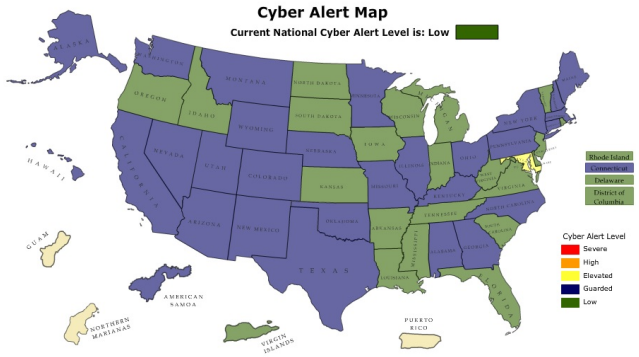
Governor's Cybersecurity Dashboard

MAY 2015

MAJOR CYBER INCIDENTS

CIS / MS-ISAC's cyber threat map:



State agencies, critical infrastructure & private sector cyber threats:

Reported cyber incidents	Affected entities	Impact
• Severe impact:	• Retailer	• Name, address, SSN, pmt. card info, email address; malware; 1855 affected
• High impact:		
• Elevated impact:	• Financial Services	• Name, address, credit card info, email, user credentials; hacking; 155 affected
	• Manufacturer	• Name, credit card info; malicious code; 109 affected
	• Financial Services	• Name, address, SSN, benefits plan, pmt & bank info; inadvertent disclosure; 10172 affected
	• Manufacturer	• Name, email address, phone no, credit card info; phishing attack; 210 affected
	• Contractual services	• Name, address, SSN, bank info; unauthorized access; 1892 affected

CYBERSECURITY PROGRAM

Call-to-action on state cybersecurity:

Action	Status	Progress
1. State cybersecurity governance & authority	Continuing	—
2. Cybersecurity awareness & cyber culture	On track	▲
3. Continuous monitoring for threats & vulnerabilities	On track	▲
4. Best practices (e.g. NIST Cybersecurity Framework and Council on Cybersecurity (CSS) 20 critical security controls)	Continuing	Mapping agency assessment findings to Critical Controls

State cybersecurity initiatives:

Description	Status	Progress	Cost	Completion date	Milestones
1. Cybersecurity services/personnel contract	On track	▲	$7.5M NTE	8/14/2013	Contract awarded
2. Standardized statewide cyber security training	On track	▲	$160K annually	8/23/2013 10/29/2014	Contract awd; 42K enrollees Year 2 option exercised
3. Statewide incident response planning	On track	▲	TBD	5/31/2015	Agency checklists, workflows in development

CYBERSECURITY MONTHLY REPORT CARD

Top 5 risks & significant threats:

1. Personally identifiable information (PII) and protected health information (PHI) systems and data require improvements in classification, assessment, monitoring, scanning and maintenance.
2. More sophisticated and better crafted phishing campaigns put statewide users at higher risk of giving up valuable identification credentials and/or data. Increasing vigilance is required.
3. Absence of and/or untimely patching and updating of hardware platforms, operating systems and applications exposes vulnerabilities and opportunities for malicious exploitation.
4. Includes numerous anomalies: Deviation from SOPs, data handling errors, poor computer hygiene, theft/loss of equipment, etc.
5. Statewide: Submission of annual security plans establishes baseline, but collectively requires continuous improvement.