



Homeland Security
and Emergency Services

**Cyber
Security Grant Program
&
DHSES Cyber Initiatives**

November 6, 2019

Agenda

- ✓ ***Overview of DHSES cyber teams***
 - Cyber threat overview
 - Grant objectives
 - Allowable costs
 - Cyber security grant program changes



Mission Objectives



Identify / Prevent / Protect

- Cybersecurity toolkit
- Training and exercises
- Outreach to customer base
- Community of practice
- Vulnerability scanning

Respond / Recover

- Incident response and digital forensics
- Remediation assistance

Agenda

- Overview of DHSES cyber teams
- ✓ ***Cyber threat overview***
- Grant objectives
- Allowable costs
- Cyber security grant program changes



Threat Overview

- Ransomware attacks are on the rise:
 - Most common type of cyberattack for city/county governments
- Phishing tactics (e-mail based) are the most common methods for successful cyberattacks
- Attempted, even successful attacks, often go unnoticed
- Most jurisdictions have limited cyber security policies and response plans
 - Funding levels are often not adequate as threats continually evolve in frequency and sophistication



Agenda

- Overview of DHSES cyber teams
- Cyber threat Overview
- ✓ ***Grant Objectives***
- Allowable costs
- Cyber security grant program changes



Objectives

- To provide local jurisdictions with the resources and equipment necessary to prevent disruption of the confidentiality, integrity, and availability of their information systems
- To assess cyber risks, identify vulnerabilities and determine capability gaps with the focus of allocating resources to address the most critical needs
 - Risk assessment tools are embedded in the grant application process
 - Proposed projects should address identified risks



Objectives (cont.)

- To ensure that local jurisdictions are equipped with the knowledge and resources necessary for providing cyber security awareness training to their staff in support of good cyber hygiene at the user level
- To develop actionable Cyber Security Plans that focus on response and immediate remediation to a cyberattack
 - Cyber security exercises
 - Provides opportunities to implement and evaluate the effectiveness of existing cyber security response plans
 - Outcomes can identify vulnerabilities; where to focus enhancement/investment



Objectives (cont.)

- Encourage the participation in established cyber security support networks and utilization of the vast amount of resources available to local governments



MS-ISAC[®]
Multi-State Information
Sharing & Analysis Center[®]



Homeland Security
and Emergency Services

Agenda

- Overview of DHSES cyber teams
- Cyber threat overview
- Grant objectives
- ✓ ***Allowable costs***
- Cyber security grant program changes



Allowable Costs

- **Planning**
 - Costs associated with the development of plans to include the hiring of consultants to identify potential vulnerabilities and develop risk mitigation plans
- **Equipment:**
 - Hardware updates that will provide protection against cyber threats
 - Software packages including firewalls, anti-virus/malware protection
 - Intrusion detection systems



Allowable Costs (cont.)

- **Training:** costs associated with development and delivery of cyber awareness training programs
- **Exercises:** costs associated with the development, execution and evaluation of cyber security exercises



Unallowable Costs

- **Organizational costs**
 - Hiring of full/part-time staff
- **Management and Administration Costs (M&A)**
 - OT/backfill costs, facility rent/lease, office supplies, etc.
- **Construction costs**



Agenda

- Overview of DHSES cyber teams
- Cyber threat overview
- Grant objectives
- Allowable costs
- ✓ ***Cyber security grant program changes***



Cyber Security Grant Changes

- **Primary changes for the FY 2019**
 - New self assessment based on the CIS Critical Security Controls
 - New requirement to complete the Nationwide Cyber Security Review NCSR, if you are awarded funding.



FY 2017-18 Self Assessment

FY2017 Cyber Security Targeted Grant Program

2. Risk Level Self-Assessment

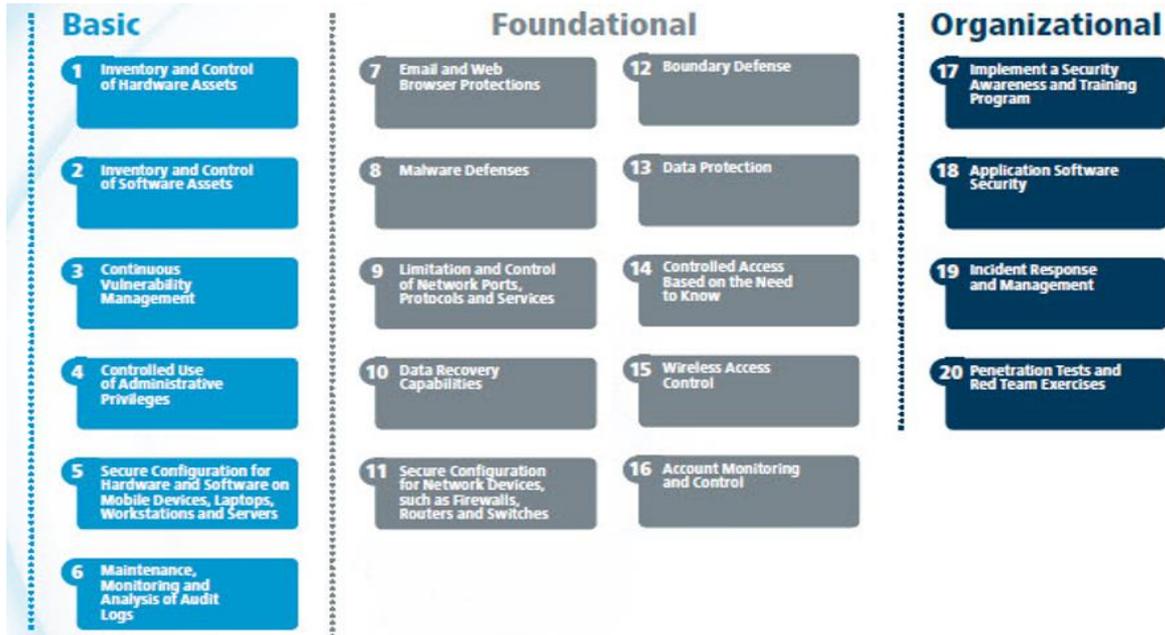
Please select one response per row for the questions below. Select the response that most closely describes the security of your cyber-systems. Select only one response per row. Proposed projects should address the higher risk areas identified on this worksheet unless further justification is provided in the "Capability Advancement" section. All three components of the Risk Assessment ("Self-Assessment", "Posture Survey" and "Threat Profile") will be evaluated and scored as a whole and will be worth a maximum of 30 points.

	Question	Optimized Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness	Implementation In Progress Your organization has formally documented policies, standards, and procedures	Documented Policy Your organization has a formal policy in place	Informally Performed Activities a processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented	Not Performed Activities, processes and technologies are not in place to achieve the referenced objective
1	Devices and software (including externally managed systems) are inventoried and classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Vulnerability scans are performed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Permissions are managed and provided based on the principles of least privilege	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Privileged users understand roles & responsibilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Organizational information security policy is established	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	All users are informed and trained	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Data at rest and in transit is protected	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



FY 2019 Self Assessment

Organizations that apply just the first 5 CIS Controls can reduce their risk of cyberattack by around 85 percent. Implementing all 20 CIS Controls increases the risk reduction to around 94 percent.—CIS.org



CIS Top 20 Security Controls



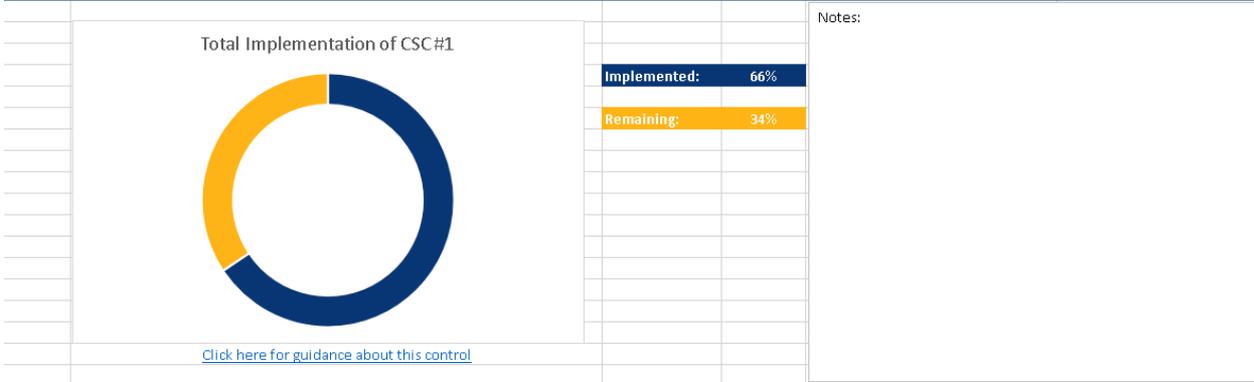
FY 2019 Self Assessment



NEW YORK STATE

Homeland Security and Emergency Services

Critical Security Control #1: Inventory and Control of Hardware Assets



Notes:

ID	Critical Security Control Detail	NIST CSF	Group	Sensor or Baseline	Control Implemented
1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	Identify	2	Active Device Discovery System	Implemented on All Systems
1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	Identify	3	Passive Device Discovery System	Not Applicable Not Implemented Parts of Control Implemented Implemented on Some Systems Implemented on Most Systems Implemented on All Systems
1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	Identify	2	Log Management System / SIEM	Implemented on All Systems
1.4	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	Identify	1	Asset Inventory System	Implemented on All Systems



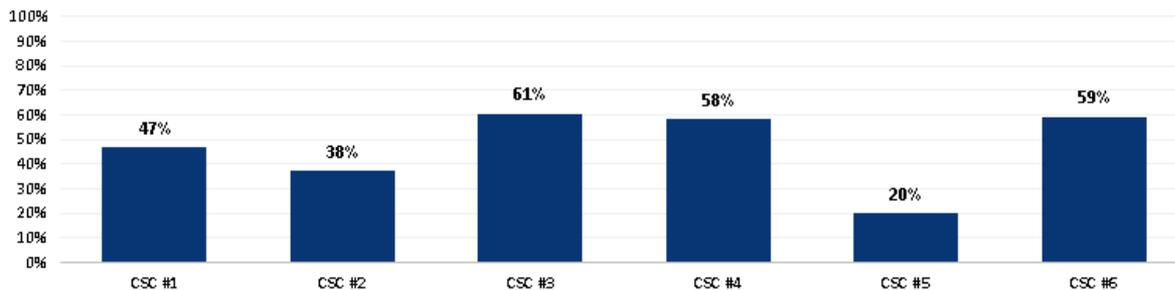
Overall Implementation - Basic Controls



What is this chart telling me?

The Overall Implementation - Basic Controls chart shows the degree to which the "Basic 6" CIS Critical Security Controls have been implemented at your organization. Whether the level of implementation is supported by organizational policy, the controls are automated, or are reported to organizational management are not reflected in this chart.

Basic Control Compliance by Control



What is this chart telling me?

The Basic Control Compliance by Control chart shows the degree of implementation for each of the "Basic 6" CIS Critical Security Controls, individually.



Nationwide Cyber Security Review (NCSR)

General Overview

- **NEW** Requirement for all FY2019 SHSP and UASI Recipients and Sub-Recipients
 - Outlined in Information Bulletin (IB) No. 439, issued April 12, 2019
 - Condition to receive funding
- No cost, anonymous annual self-assessment designed to measure gaps and capabilities of governments' cyber security programs
- Enables entities to benchmark and measure progress of improving cyber security posture
- Hosted by Multi-State Information Sharing and Analysis Center (MS-ISAC) – Provide Technical Assistance



Nationwide Cyber Security Review (NCSR)

Important Tips and Reminders

- CIO/CISO or most senior Cyber Staff should complete the NCSR
- Must be completed by **December 31, 2019**
- Guidance was E-Mailed via DHSES Grant Info on 9/19/19
- Informational Webinar held on 9/20/19; Next Webinar will be 11/1/19
- All Webinars will be posted on the MS-ISAC website
- For more info: <https://www.cisecurity.org/ms-isac/services/ncsr/>



Contact Information

- **Contact Critical Infrastructure Protection (CIP)**
 - To request service, please email us at: CIP.OCT@dhses.ny.gov
 - If you have questions please call:
 - Kurt Osterman: 212-849-4469
- **Contact DHSES Cyber Incident Response Team (CIRT)**
 - To report a cyber incident please call: 1 (844) OCT-CIRT | 1 (844) 628-2478
 - To request DHSES CIRT cyber support please email: CIRT@dhses.ny.gov
 - <http://www.dhses.ny.gov/oct/cirt>
- **Contact DHSES Grants Program Administration (GPA)**
 - Grants hot line: 1-866-837-9133
 - E-Mail: Grant.Info@dhses.ny.gov
 - Website: <http://www.dhses.ny.gov/grants/>

Questions?

