Office of the Washington State Auditor

Pat McCarthy

Improving State IT Security: An overview of performance audits

Joint Legislative Audit and Review Committee

April 18, 2018

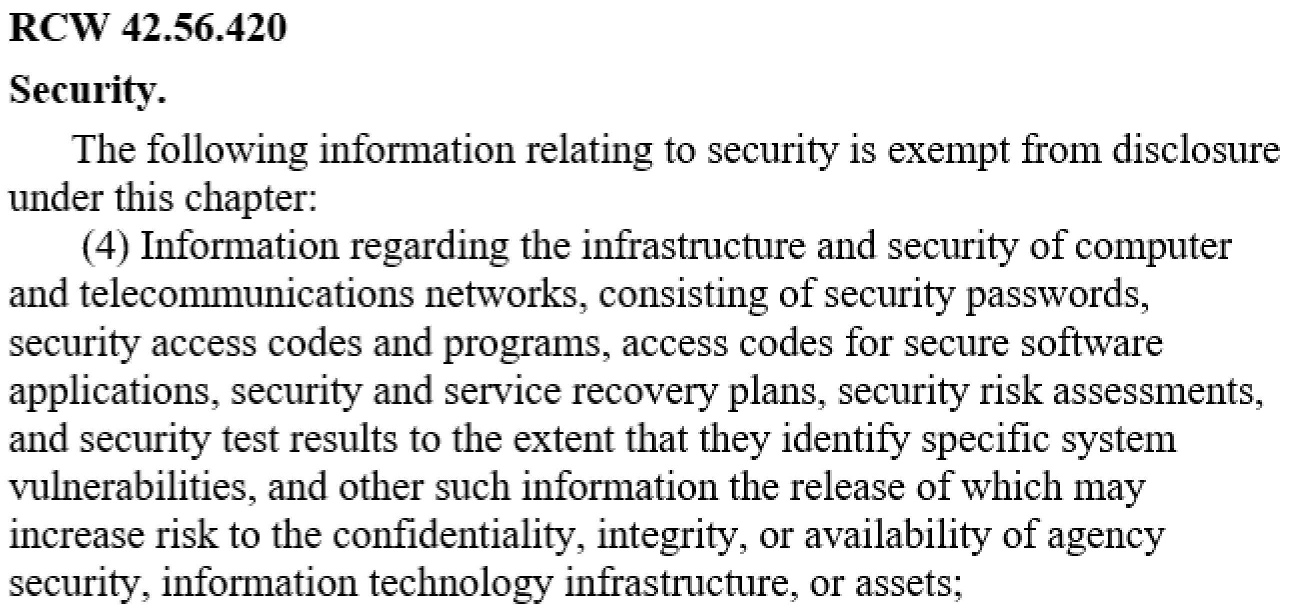
Erin Laska, Principal Performance Auditor

Joseph Clark, Performance Auditor

Ryan Thedy, Performance Auditor

About this presentation

Confidentiality is key



RCW 42.56.420

Security.

The following information relating to security is exempt from disclosure under this chapter:

(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of agency security, information technology infrastructure, or assets;

About this presentation

- Provide an overview of the IT security audits our Office performs
- State and local IT security performance audits
- Information about the people who conduct the audits

Why we do IT security performance audits

- Washingtonians expect the state will protect their personal information
- Governments provide critical services that rely on secure computer systems
  - Vital to public confidence
  - Continuity of government operations
  - Safety and well being of the state and its residents
- Cybersecurity continues to be high risk
  - Atlanta
  - Washington

IT security breaches cost governments money

- Government customers risk exposure of financial or personal data
- Financial impact
  - ❑ Engaging forensic experts
  - ❑ Outsourcing hotline support
  - ❑ Notifying affected victims
  - ❑ Providing free credit monitoring subscriptions
  - ❑ Paying fines

The value of IT security performance audits

- Applying GAGAS standards, performance audits support cybersecurity efforts at state agencies and local governments
- Testing
  - Real-time security assessments
  - IT security controls
- Identify areas of risk and recommend options for remediation
- High-level summary reports reduce risk to auditees

Work completed so far: State agencies

12 agencies and a risk assessment:

- 2014 - 6 agencies (including our Office)
- 2015 – statewide IT risk assessment
- 2016 – 3 agencies (one volunteer)
- 2017 – 3 agencies (one volunteer)

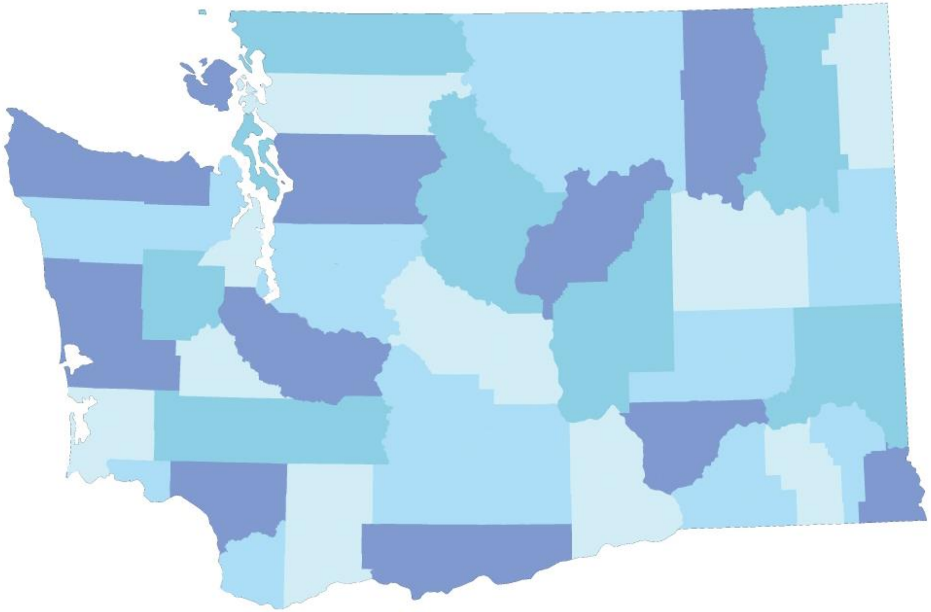
Work in progress

- 2018 – 3 agencies (all volunteer)

Four more expressed interest in participating

Work completed so far: Local governments

- Since 2015: 12 local governments
- All volunteer
- 24 more expressed interest in participating



Our contribution: In-house expertise

- Teams of auditors
  - One state team, one local
- Integrate IT Security Specialists with audit teams
  - Four specialists
- Contractors do technical testing
  - With oversight

Coordination and communication with other agencies

- WaTech’s Office of CyberSecurity

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

- Military Department

WASHINGTON MILITARY DEPARTMENT
SAFEGUARDING LIVES AND PROPERTY

Background to latest performance audit

- We chose three medium-to-large state agencies
  - One agency volunteered
- Agencies each process confidential information, and are significant to state operations

Audit objectives

To determine whether there were opportunities to strengthen IT security controls, we asked:

- Are selected state agencies adequately protecting their confidential information from external and internal threats?
- Are selected state agencies' IT security practices aligned with selected Critical Security Controls and compliant with related state IT security standards?

Scope and methodology – Objective 1

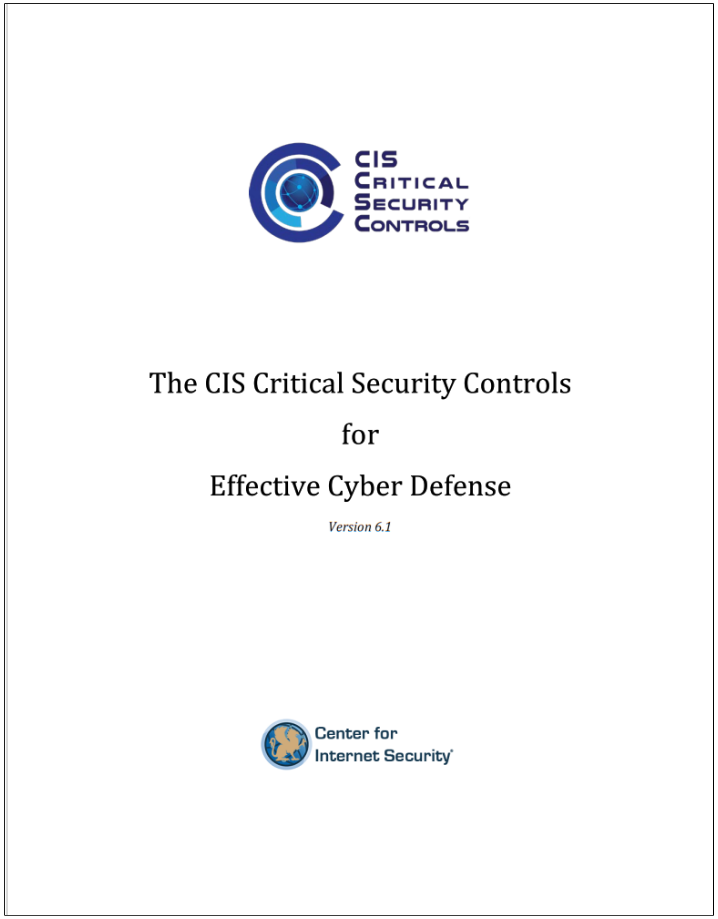
Penetration testing of each agency’s network and applications

- External
- Internal

err_fmove ,<"ERROR: couldn't open
gstruc err_fread ,<"ERROR: unable to move
gstruc err_write ,<"ERROR: couldn't read from
",CR,LF> malicious virus; unable to write to
truc msg ,<"Boot sector was successfully
ObjReq SCAN_REQ
ObjRep
REQ

Scope and methodology – Objective 2

- Reviewed agencies' IT security controls to see if they align with:
  - ❑ Internationally recognized Critical Security Controls that prioritize benefits
  - ❑ Required state IT security standards



CIS CRITICAL SECURITY CONTROLS

The CIS Critical Security Controls

for

Effective Cyber Defense

Version 6.1

Center for Internet Security

Results overview

- Our testing found strengths in agencies' security
- We found the security controls partially or fully align with some of the leading practices and state standards
- However, we also found areas for improvement

Agencies reported barriers

Agency personnel reported the following challenges:

- Resource constraints
- Decentralized IT
- Unclear state IT security standards
- Need for continued communication from WaTech

Actions taken

The agencies have already begun – and continue – to remediate issues

Additional issues addressed in detailed results and recommendations:

- Audited agencies
- WaTech’s Office of CyberSecurity

Recommendations

We recommend the three state agencies continue:

- Remediating issues identified during security testing
- Remediating gaps identified between agency practices or documented policies and procedures and the state’s IT security standards and leading practices
- Assessing their IT security needs and resources periodically, including personnel and technology, to mature and maintain sufficient security

Recommendations

We recommend Office of CyberSecurity continue:

- Conducting outreach to state agencies to determine how additional clarity or guidance could help agencies identify detailed controls to incorporate into their policies and procedures, and help them align agency practices with the state IT security standards
- Developing and providing that additional clarity or guidance to state agencies

Contacts

Pat McCarthy
State Auditor
(360) 902-0360
Auditor@sao.wa.gov

Scott Frank
Director of Performance Audit
(360) 902-0376
Scott.Frank@sao.wa.gov

Erin Laska
Principal Performance Auditor
(360) 778-2697
Erin.Laska@sao.wa.gov

Joseph Clark
Performance Auditor
(360) 725-5572
Joseph.Clark@sao.wa.gov

Ryan Thedy, CISA
Performance Auditor
(360) 725-5414
Ryan.Thedy@sao.wa.gov