



Virginia Information Technologies Agency

# Cyber Security Update

**Mike Watson**

Commonwealth Chief Information Security Officer

---

CIO Council

May 8, 2013





## Overview

- Review previous discussion
- Update security data
- Discuss the road forward
- Questions



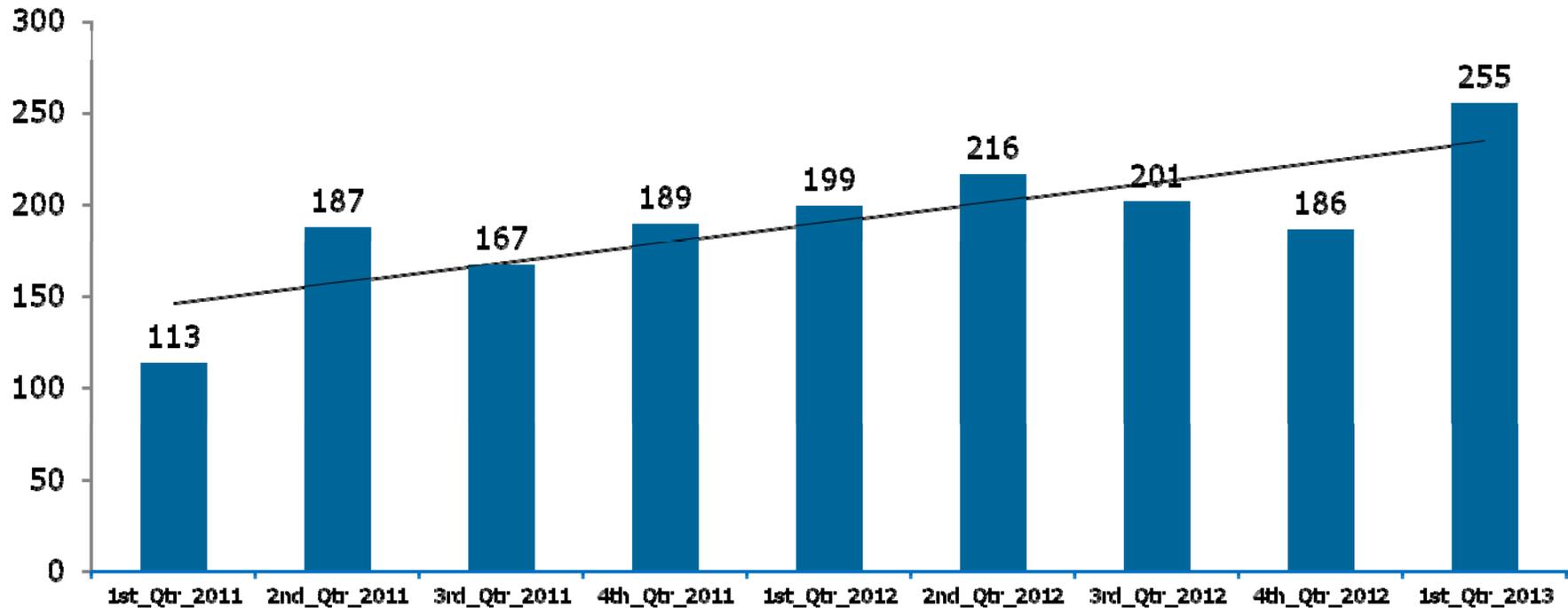
## March Meeting Highlights

- Presented agency security data
  - Risk management program data
  - Security audit program data
  - Agency threat data
- Discussed operational security issues
  - Local admin rights (LAR)
  - Windows 2000
  - SQL 2000
- Discussed how to help
  - Requested help to get agency head attention



# COV Cyber Security Incidents

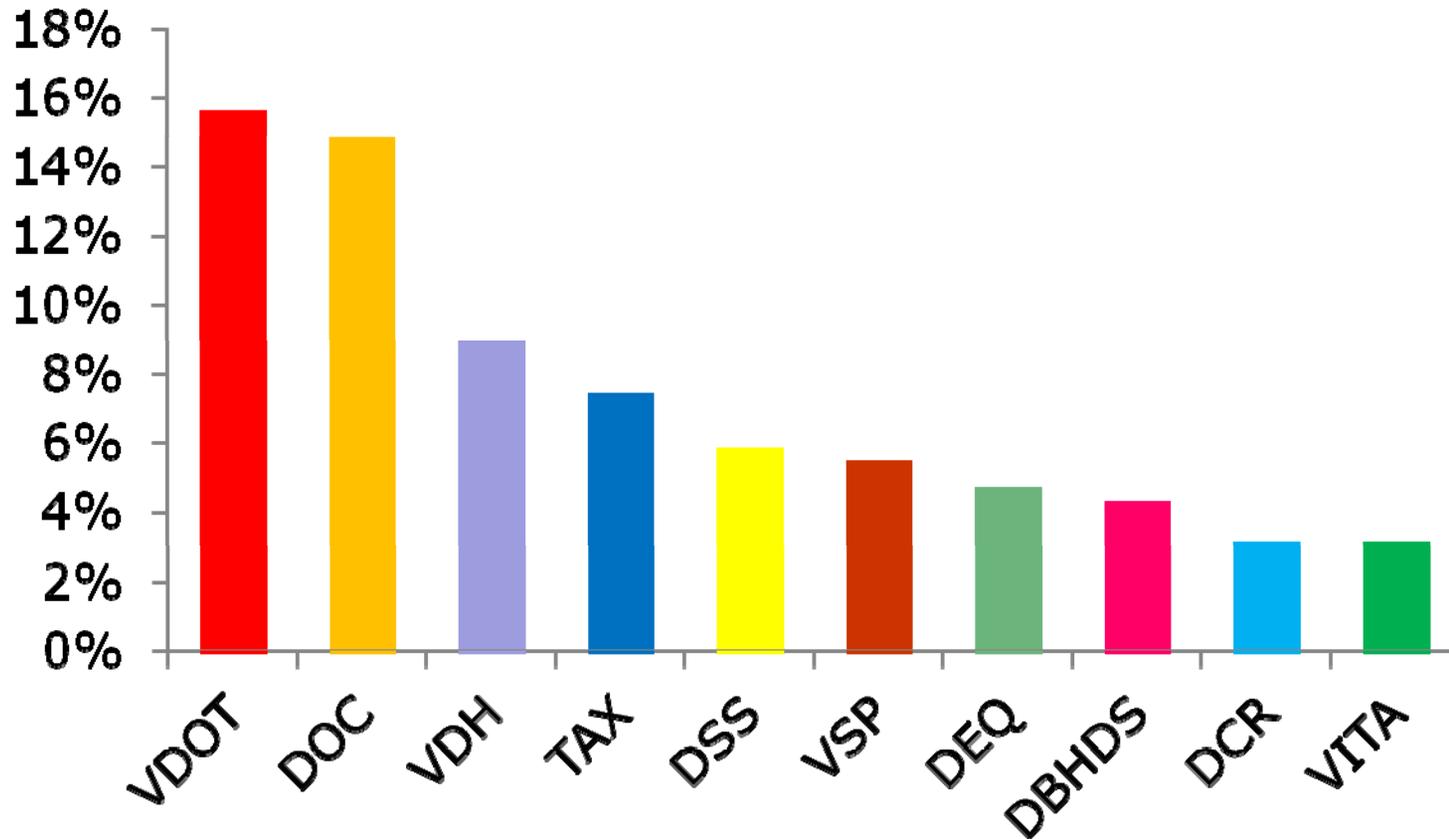
Incident Trends by Quarter  
2011 - 1<sup>st</sup> Qtr 2013





## Security Incidents by Agency – 1<sup>st</sup> Qtr 2013

**Percentage of Total Incidents**





## Recent Cyber Incidents

- Denial of service attacks (DNS)
  - Attacks against DNS servers
  - Amplification attack
    - Small packet request -> large packet response
  - Rate limiting put into place
  - Prepared for additional attacks
- OpUSA
  - No direct threats against COV assets
  - Denial of service attacks likely
  - Primarily targeting financial and government sites



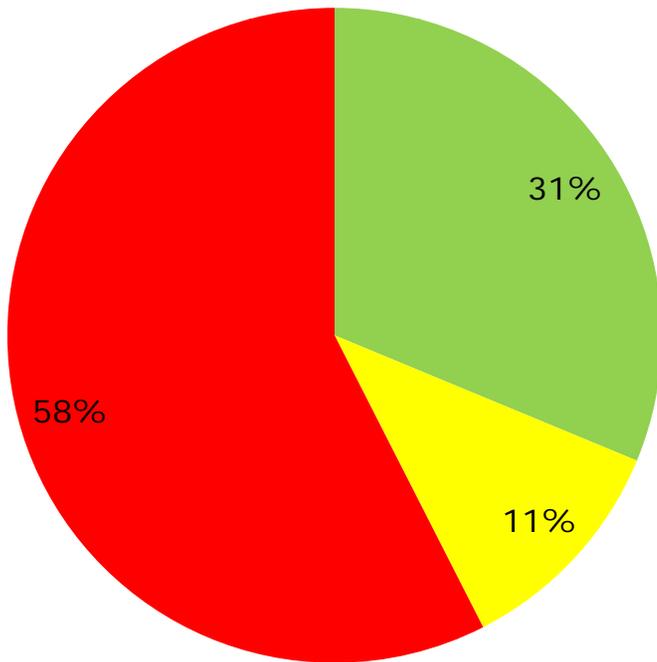
## Operational Security

- LAR
  - Some progress
- Out-of-support software security controls
  - Windows 2000
  - SQL 2000
- JAVA progress
  - Packaging second to latest version
    - Planned availability – week of May 20th
  - New auto-uninstall behavior extended testing

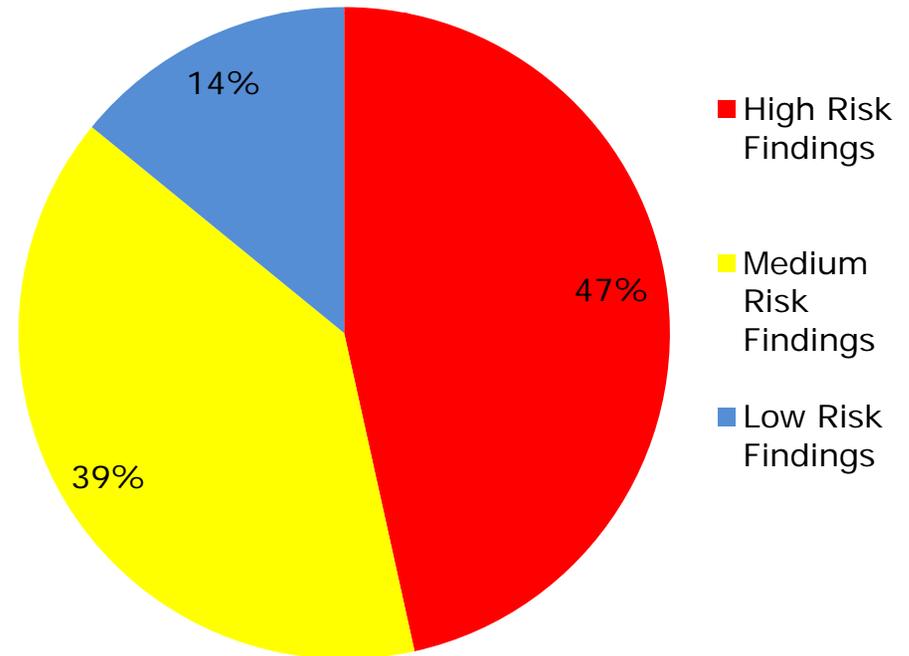


# Annual Report Data Points

### Commonwealth Overall Audit Program Score



### Risk Assessment Findings



- High Risk Findings
- Medium Risk Findings
- Low Risk Findings



## Risk Management - Risk Capture Process

- Identify risk and plan for treatment
  - ISO/AITR notified of risk identified
  - Risk treatment plan
    - Two weeks – high
    - Four weeks – medium
    - Six weeks – low
- Risk treatment plan
  - Plan to remediate risk
  - Within 90 days of notification



## Risk Management – Notification Process

- First Notification
  - ISO/AITR
  - Includes information surrounding the risk and the request for a plan
- Second notification
  - ISO/AITR
  - Agency head
  - Additional request for plan
- Final notification
  - Secretary
  - Includes possible agency impacts
    - Includes estimated costs
    - Includes any impact to agency IT procurement



## Risk Management Process - Goals

- Understand risk carried
- Apply resources to highest risk issues
- Assist with top down support
- Identify high-risk systems



Virginia Information Technologies Agency



# Questions?

