The Cost of Cybersecurity for IT Systems

FY20 Joint Information Technology and Software Cost Forum

15-17 September 2020

Dan Harper (The MITRE Corporation)

Richard Mabe (PRICE® Systems, LLC)

Bottom Line Up-Front

1. **Cybersecurity costs are not well understood, but a lot can be learned by studying Federal IT System data reported via the public Office of Management and Budget (OMB) IT Dashboard**
   - Includes rich set of spending/budget data for cyber factors (but not CERs)
2. **Enough data to identify Benchmarks/Factors to use for estimating**
   - Cyber $ costs as % of Total Investment Program Expenditures
   - Cyber metrics
3. **Disparate data could be mapped into “Cyber Cost Categories” to establish factors by logical groupings**
4. **Cyber costs included 5 categories consistently; roughly a dozen others as “spikes”**

Overview

- Cybersecurity Costs: Definition and Cost Elements
- Cybersecurity as part of an IT System
- Cybersecurity as an IT System Primary Function

Cybersecurity Definition

- **Cybersecurity includes measures taken to:**
  - Protect digital devices, processors, systems and networks against unauthorized access or attack
  - Protect against information being lost, stolen or compromised
  - Protect confidentiality, integrity and availability of data and systems
- **Cybersecurity includes hardware and software technology, as well as policy-based strategies**

Cybersecurity Cost Elements

- **Hardware***
  - Cybersecurity Functions: Monitor, Control, Mitigate, Protect, Attack
  - Mostly COTS items (Routers, Switches, Firewalls, Servers, Intrusion Detectors, Scanners, Filters)
- **Software***
  - Cybersecurity Applications: Protect, Filter, Monitor, Mitigate, Control, Alert, Counter-act
  - Mostly COTS items (Anti-virus, Spyware, Malware, Anti-Ransom, Anti-Phishing, Network Control/Monitor, Filters, Firewalls)
- **Labor Effort**
  - Determine requirements and solutions (on-going engineering process for life cycle)
  - Procure, Modify, Validate, Test, Certify, Operate/Monitor, Update as requirements change
  - Labor Categories that apply to the Cyber domain
    - System Engineers, Software Engineers
    - IT Managers, Data Administrators, Network Managers/Controllers
    - Cyber Technicians/SMEs, Test Engineers and Technicians

** Configuration depends on host platform: Weapon System, Data Center, Commercial Cloud*

I. Cybersecurity as part of an IT System

Scope

- **Focus on cost categories identified in Mil-Std-881D (Work Breakdown Structures for the DOD)**
  - Hardware, Software, and Services
  - Life cycle engineering and cybersecurity management
- **Cost and Budget source data summarized from the OMB IT Dashboard**
  - Executive branch (cabinet) agencies and programs
  - Business systems
- **Present normalized data analysis results as factors to use in cost estimating**
  - Cyber Activity Cost = % of Other Program Cost or Technical Values

Background, Methodology and Approach

- **Initial database from the OMB IT Dashboard included 16,380 IT activities**
  - Develop SW; Buy and Integrate HW; Prepare documentation; Complete risk assessments; etc.
  - 568 Individual IT Systems represented
  - Across 25 Executive Branch Agencies
- **Identified cybersecurity activities and related costs**
  - Based on expenditures by IT System development and support activity (FY09 – FY16)
- **Filtered the data by keywords found within the funded activity definitions to isolate cybersecurity related activities**
  - For example: Cyber, Security, Vulnerability, Detection, Certification, Penetration, Incident
- **Initial data set for analysis:**
  - 615 cybersecurity-related activities
  - Within 165 Individual IT Systems
  - Across 22 Executive Branch Agencies

Survey Question

- Do you think there is correlation between activity costs within agencies or between agencies?
  - Yes
  - No

IT Dashboard Data Limitations

- Dataset did not include DOD IT Systems
- Costs not identified by Appropriation or by Labor Category
- Unable to identify split between contract labor and government employees
- Did not normalize Then-Year $ to Constant Base Year $
- Representative sample; using additional keywords resulted in duplicate activities

Analysis Approach

1. **Created "Cyber Cost Categories" to establish factors by logical groupings; for example:**

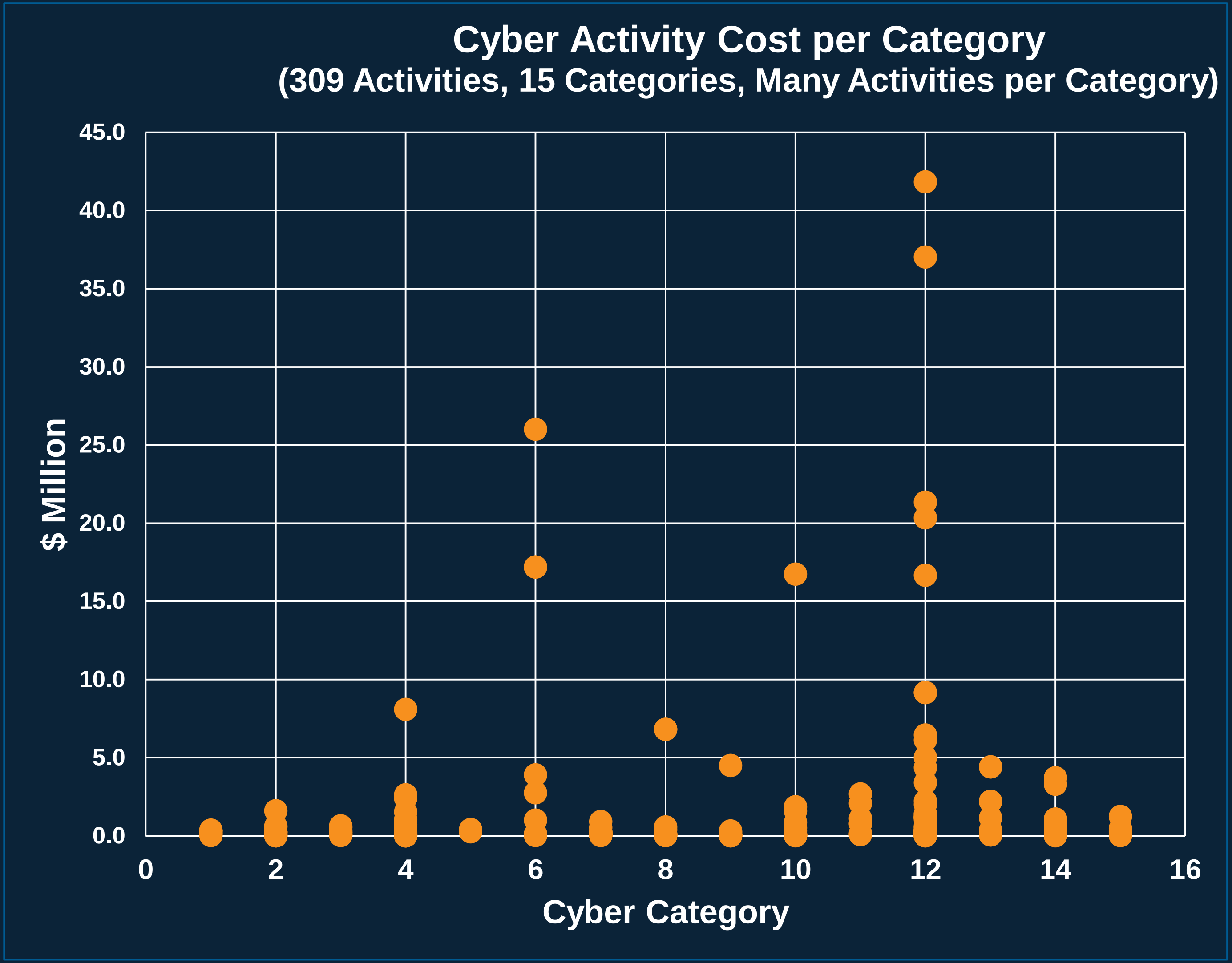
Management	Requirements/Risk	HW/SW
Manage Cyber Program	Authentication/Certification	SW Application Release
Contractor Support	Architecture/Design	SW Maintenance Release
Cyber Testing	Cyber Requirements Analysis	Security Patch/IAVA
Cyber Documentation	Assess Risk/Manage Controls	Cyber HW Procure
Cyber Training	Assess Security (General)	Cyber HW Maintain
		Cloud Costs/Fees

2. **Further filtered out activities containing "mixed" data including both cybersecurity and non-cybersecurity costs and effort**

3. **Remaining database size and content sorted by Cyber Cost Category:**

   - 309 cybersecurity activities within 34 Individual IT Systems across 21 Executive Branch Agencies

Cyber Activity Cost per Category



Cyber Categories

1 Architecture/Design
2 Assess Risk/Controls
3 Assess Security (General)
4 Authentication/ Certification
5 Cloud Costs/Fees
6 Contractor Cyber Support
7 Cyber Documentation
8 Cyber HW Procure
9 Cyber Requirements Analysis
10 Cyber Testing
11 Cyber/Security Training
12 Manage Cyber Program
13 Security Patch/IAVA
14 SW App Release
15 SW Maint Release

Analysis Findings

- **No correlation between activity costs within agencies or between agencies (Excel, TrueFinding®)**
  - Spending for cybersecurity activities varied widely by Executive Agency and IT System
  - Spending appeared to be random (tailored by individual agency and IT System)
- **Could not establish valid CERs**
  - So: Evaluated data to identify Benchmarks or Factors to use for estimating
    - Cyber $ costs as % of Total Investment Program Expenditures

Results: Most Frequent Cyber Elements and Cost Drivers

1. **Manage Cyber Programs, Authentication/Certification and SW App Releases are the most prevalent cyber activities (green font)**
   - Represent 50% of all Cyber activities (152 of 309 Total)
   - But only 6% on average of Total Investment Cost
   - Pervasive in many programs, but not cost drivers

2. **Contractor Cyber Support and Cyber/Security Training are cost drivers (red font)**
   - Highest Avg % of Total Investment Cost
   - But they represent only 7% of all cyber activities
   - Only drivers when they occur

Cyber Activity	Number of Activities by Category	% by Category (309 Activities)	Avg % Total Program Cost
Manage Cyber Program	69	22%	2.19%
Authentication/ Certification	43	14%	1.18%
SW App Release	40	13%	2.58%
Cyber Documentation	21	7%	0.78%
Assess Security (General)	21	7%	1.49%
Cyber Testing	17	6%	2.33%
Security Patch/IAVA	15	5%	0.89%
SW Maint Release	14	5%	2.13%
Cyber Requirements Analysis	14	5%	0.70%
Assess Risk/Controls	13	4%	1.73%
Contractor Cyber Support	11	4%	7.64%
Cyber HW Procure	10	3%	4.78%
Architecture/Design	10	3%	1.44%
Cyber/Security Training	8	3%	10.30%
Cloud Costs/Fees	3	1%	1.55%

Conclusions (Cyber Elements and Cost Factors)

Cyber Activity	Number of Activities by Category	Average % Total Program Cost	Median % Total Program Cost	High % Total Program Cost	Low % Total Program Cost
Manage Cyber Program	69	2.19%	0.27%	33.72%	0.001%
Authenticate/Certification	43	1.18%	0.42%	12.03%	0.01%
SW App Release	40	2.58%	0.71%	16.77%	0.01%
Cyber Documentation	21	0.78%	0.27%	5.82%	0.04%
Assess Security (General)	21	1.49%	0.96%	9.37%	0.08%
Cyber Testing	17	2.33%	0.16%	31.01%	0.001%
Security Patch/IAVA	15	0.89%	0.42%	4.13%	0.18%
SW Maint Release	14	2.13%	1.04%	10.13%	0.03%
Cyber Reqts Analysis	14	0.70%	0.30%	5.01%	0.02%
Assess Risk/Controls	13	1.73%	1.05%	10.18%	0.07%
Contractor Cyber Support	11	7.64%	3.18%	56.52%	0.02%
Cyber HW Procure	10	4.78%	0.23%	21.62%	0.01%
Architecture/Design	10	1.44%	0.57%	10.59%	0.10%
Cyber/Security Training	8	10.30%	8.39%	29.22%	0.21%
Cloud Costs/Fees	3	1.55%	1.86%	2.52%	0.29%

Most programs include the 5 categories in green, Plus the occasional spike from the other categories

Recommendation: Use either the Sum of the Avg values for the top 5
= 8.22%
of Total Sys Cost

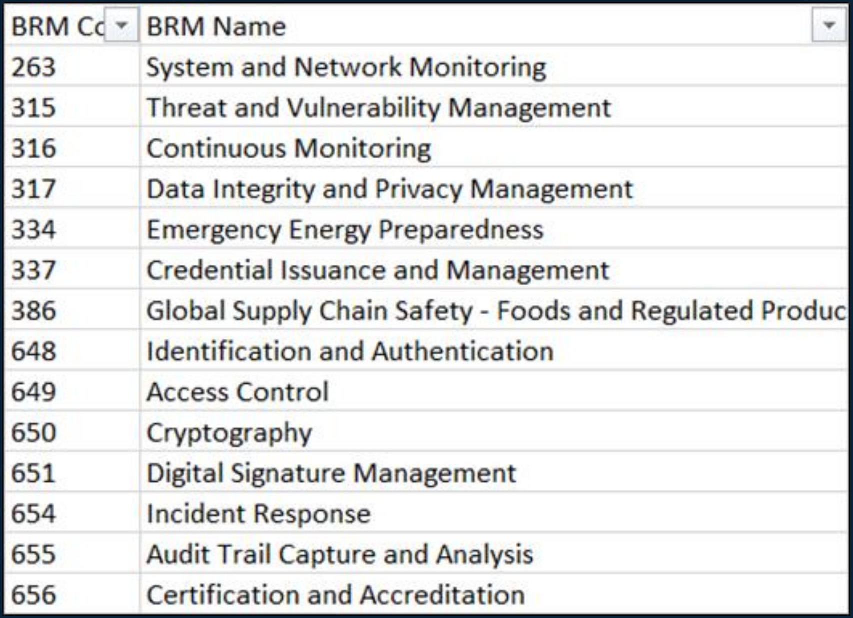
Or: the Sum of the Median values for the top 5
= 2.63%
of Total Sys Cost

Spread by % across the IT Program WBS

II. Cybersecurity as an IT System Primary Function

Approach

- IT Dashboard includes a designated Business Reference Model* Category for each IT System in the dataset
- Using BRM Definitions, determined categories that qualify as “Cyber” and used Pivot Tables to filter on any relevant IT Systems:



BRM Cc	BRM Name
263	System and Network Monitoring
315	Threat and Vulnerability Management
316	Continuous Monitoring
317	Data Integrity and Privacy Management
334	Emergency Energy Preparedness
337	Credential Issuance and Management
386	Global Supply Chain Safety - Foods and Regulated Produc
648	Identification and Authentication
649	Access Control
650	Cryptography
651	Digital Signature Management
654	Incident Response
655	Audit Trail Capture and Analysis
656	Certification and Accreditation

**BRM: Business Reference Model v3.1, Service Codes and Definitions, May 15, 2013*

316 - Continuous Monitoring

- ***Description:*** **Continuous Monitoring includes all activities related to the real-time monitoring of security controls employed within or inherited by a system (see Appendix G of NIST SP 800-37)**
- **Includes these IT Systems:**

1. DHS NPPD - Continuous Diagnostics and Mitigation (CDM)

The National Protection and Programs Directorate

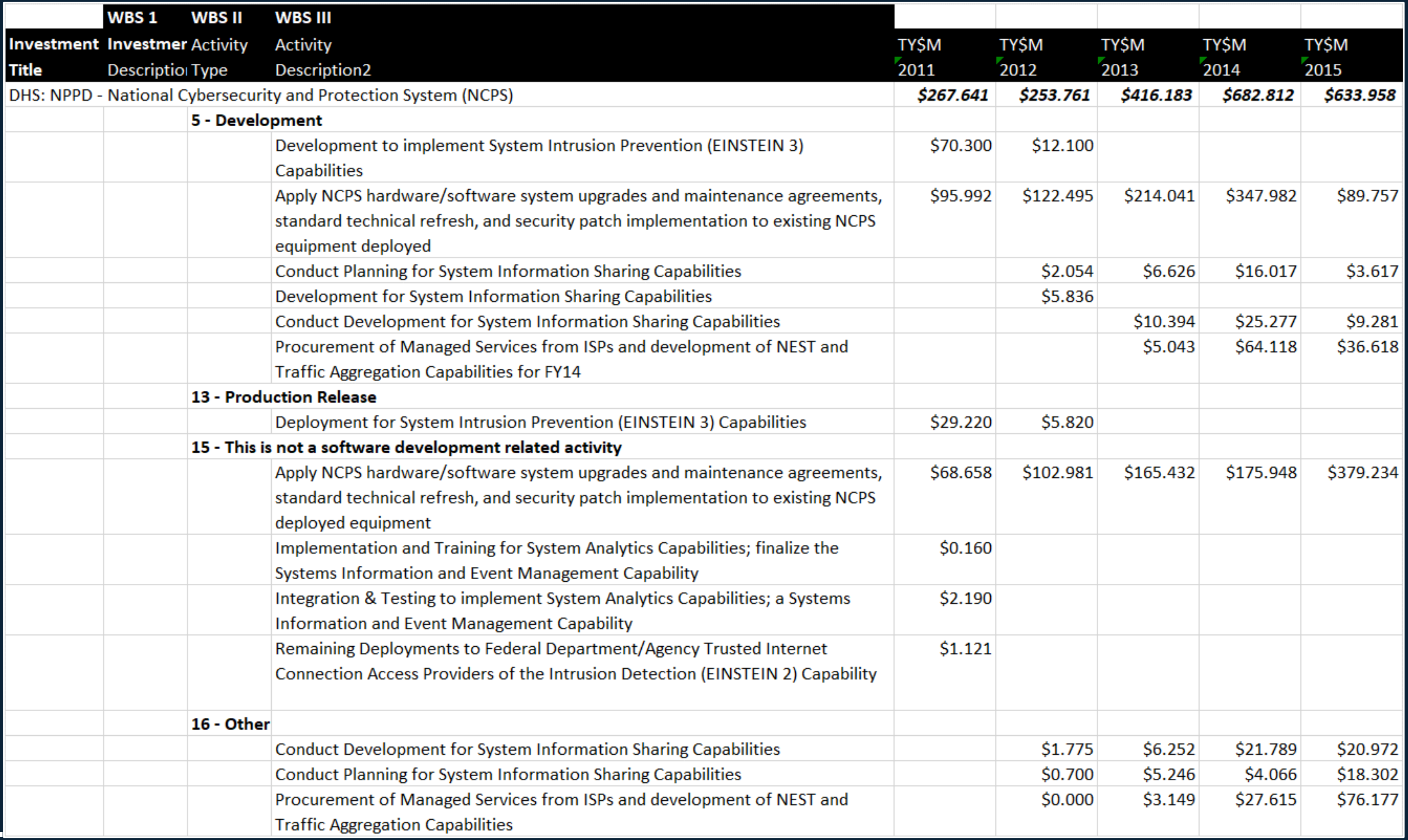
- **NPPD is a component of DHS that exists to advance the department's mission of reducing federal security risk across the country, including cyber threats and risk to communications systems**
- **Includes 5 active Investments (Systems):**
  - NPPD - Continuous Diagnostics and Mitigation (CDM)
  - NPPD - Infrastructure Protection Gateway (IPG)
  - NPPD - ISCP (Infrastructure Security Compliance)
  - NPPD - National Cybersecurity and Protection System (NCPS)
  - NPPD - Next Generation Networks Priority Services (NGN-PS)

DHS NPPD - Continuous Diagnostics and Mitigation (CDM)

- Spent $3.2M to Establish strategic sourcing vehicle
- $4.9M on CDM tools, sensors and integration services for seven agencies
- $0.9M to perform an “as is” analysis to validate its proposed CDM “as a service” (CMaaS) solution against each agency's existing infrastructure
- $0.36M to procure and deliver CDM tools and sensors to support the operation of its CMaaS Solution

DHS NPPD - National Cybersecurity and Protection System (NCPS)

Can see fairly rich level of detailed cost breakdown:



	WBS 1	WBS II	WBS III					
Investment Title	Investmer Descriptioi	Activity Type	Activity Description2	TY$M 2011	TY$M 2012	TY$M 2013	TY$M 2014	TY$M 2015
DHS: NPPD - National Cybersecurity and Protection System (NCPS)				***$267.641***	***$253.761***	***$416.183***	***$682.812***	***$633.958***
		5 - Development						
			Development to implement System Intrusion Prevention (EINSTEIN 3) Capabilities	$70.300	$12.100			
			Apply NCPS hardware/software system upgrades and maintenance agreements, standard technical refresh, and security patch implementation to existing NCPS equipment deployed	$95.992	$122.495	$214.041	$347.982	$89.757
			Conduct Planning for System Information Sharing Capabilities		$2.054	$6.626	$16.017	$3.617
			Development for System Information Sharing Capabilities		$5.836			
			Conduct Development for System Information Sharing Capabilities			$10.394	$25.277	$9.281
			Procurement of Managed Services from ISPs and development of NEST and Traffic Aggregation Capabilities for FY14			$5.043	$64.118	$36.618
		13 - Production Release						
			Deployment for System Intrusion Prevention (EINSTEIN 3) Capabilities	$29.220	$5.820			
		15 - This is not a software development related activity						
			Apply NCPS hardware/software system upgrades and maintenance agreements, standard technical refresh, and security patch implementation to existing NCPS deployed equipment	$68.658	$102.981	$165.432	$175.948	$379.234
			Implementation and Training for System Analytics Capabilities; finalize the Systems Information and Event Management Capability	$0.160				
			Integration & Testing to implement System Analytics Capabilities; a Systems Information and Event Management Capability	$2.190				
			Remaining Deployments to Federal Department/Agency Trusted Internet Connection Access Providers of the Intrusion Detection (EINSTEIN 2) Capability	$1.121				
		16 - Other						
			Conduct Development for System Information Sharing Capabilities		$1.775	$6.252	$21.789	$20.972
			Conduct Planning for System Information Sharing Capabilities		$0.700	$5.246	$4.066	$18.302
			Procurement of Managed Services from ISPs and development of NEST and Traffic Aggregation Capabilities		$0.000	$3.149	$27.615	$76.177

BRM 315 – Threat and Vulnerability Mgmt

- ***Description:*** **Involves all functions pertaining to the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction, as well as the creation and implementation of security policies, procedures and controls**
- **Includes these Systems:**

1. DHS NPPD - National Cybersecurity and Protection System (NCPS)
2. DOJ IT Security
3. DOI Infrastructure - Security Management

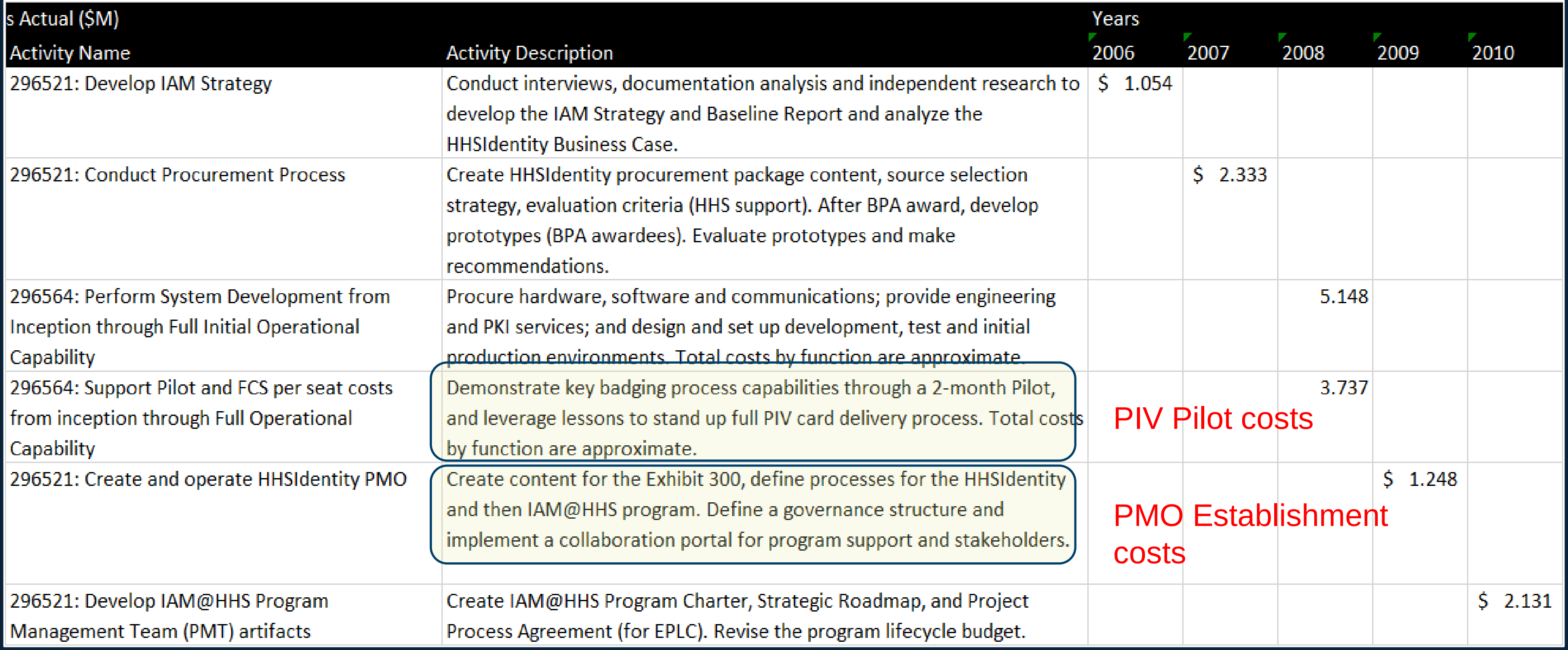
BRM 337 – Credential Issuance Mgmt

- ***Description:*** **Researching, tracking and providing of user access credentials (logical and physical) and associated security features for the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction, as well as the creation and implementation of related security policies, procedures and controls**
- **Includes these Systems:**

1. CMS Enterprise Identity Management - provide CMS Business Partners a means to apply for and receive a single User ID they can use to access many CMS applications

CMS Enterprise Identity Management (1 of 2)

- OMB IT Dashboard data very detailed, over 60 rows
- Specific tasks broken out, e.g., PIV Pilot costs; PMO Establishment costs



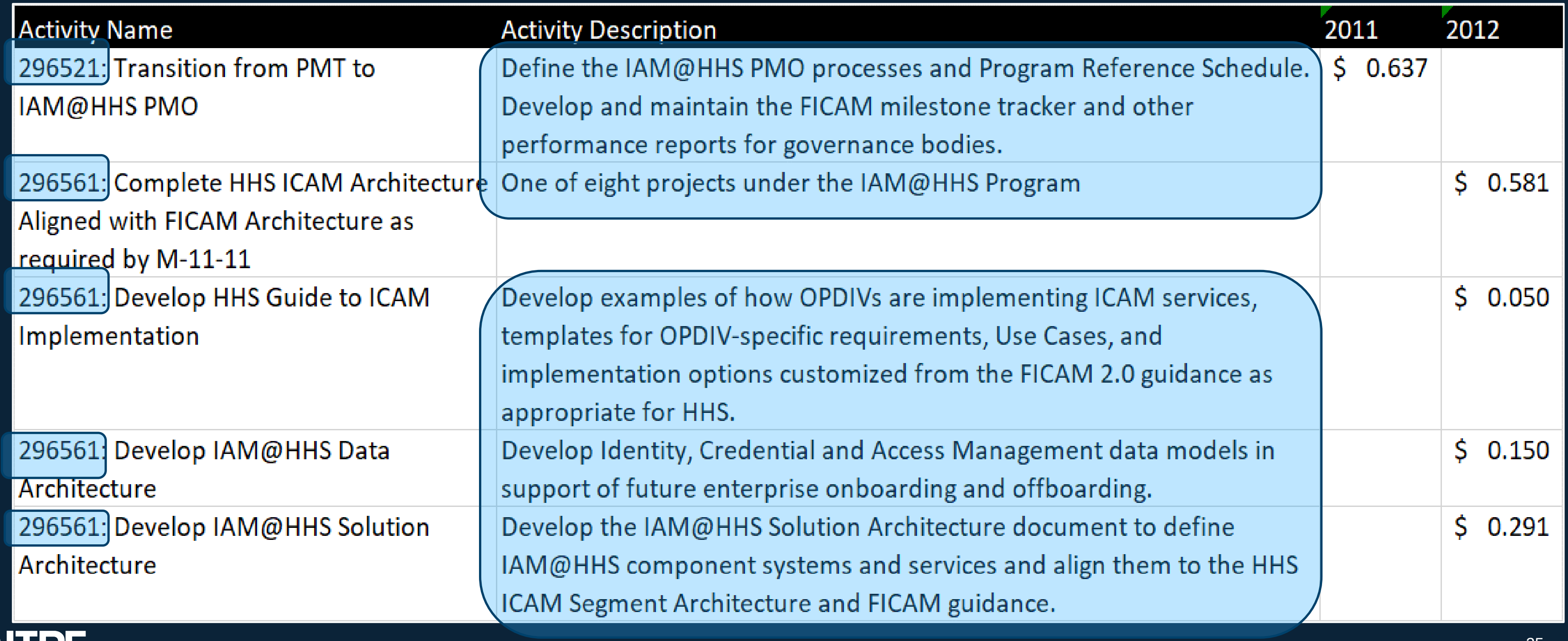
s Actual ($M)		Years				
Activity Name	Activity Description	2006	2007	2008	2009	2010
296521: Develop IAM Strategy	Conduct interviews, documentation analysis and independent research to develop the IAM Strategy and Baseline Report and analyze the HHSIdentity Business Case.	$ 1.054				
296521: Conduct Procurement Process	Create HHSIdentity procurement package content, source selection strategy, evaluation criteria (HHS support). After BPA award, develop prototypes (BPA awardees). Evaluate prototypes and make recommendations.		$ 2.333			
296564: Perform System Development from Inception through Full Initial Operational Capability	Procure hardware, software and communications; provide engineering and PKI services; and design and set up development, test and initial production environments. Total costs by function are approximate.			5.148		
296564: Support Pilot and FCS per seat costs from inception through Full Operational Capability	Demonstrate key badging process capabilities through a 2-month Pilot, and leverage lessons to stand up full PIV card delivery process. Total costs by function are approximate.			3.737		
296521: Create and operate HHSIdentity PMO	Create content for the Exhibit 300, define processes for the HHSIdentity and then IAM@HHS program. Define a governance structure and implement a collaboration portal for program support and stakeholders.				$ 1.248	
296521: Develop IAM@HHS Program Management Team (PMT) artifacts	Create IAM@HHS Program Charter, Strategic Roadmap, and Project Process Agreement (for EPLC). Revise the program lifecycle budget.					$ 2.131

PIV Pilot costs

PMO Establishment costs

CMS Enterprise Identity Management (2 of 2)

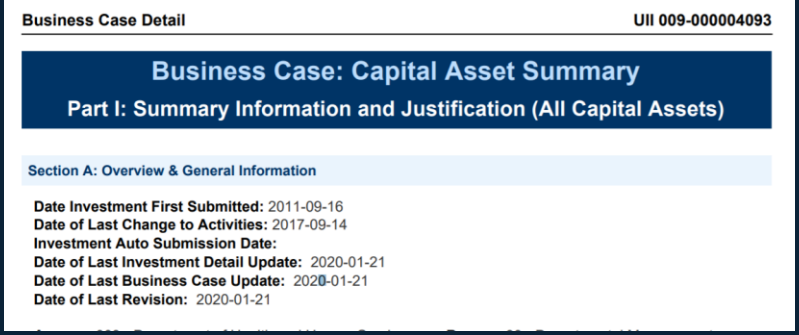
- **Detailed activity descriptions provide program insight and cost data**
- **SME not required *per se*, but helpful**
- **Machine Learning would help here; automatically parse numbers in the Activity Name field, normalize activities as WBS**
- **Actual dates for Periods of Performance also available**



Activity Name	Activity Description	2011	2012
296521: Transition from PMT to IAM@HHS PMO	Define the IAM@HHS PMO processes and Program Reference Schedule. Develop and maintain the FICAM milestone tracker and other performance reports for governance bodies.	$ 0.637	
296561: Complete HHS ICAM Architecture Aligned with FICAM Architecture as required by M-11-11	One of eight projects under the IAM@HHS Program		$ 0.581
296561: Develop HHS Guide to ICAM Implementation	Develop examples of how OPDIVs are implementing ICAM services, templates for OPDIV-specific requirements, Use Cases, and implementation options customized from the FICAM 2.0 guidance as appropriate for HHS.		$ 0.050
296561: Develop IAM@HHS Data Architecture	Develop Identity, Credential and Access Management data models in support of future enterprise onboarding and offboarding.		$ 0.150
296561: Develop IAM@HHS Solution Architecture	Develop the IAM@HHS Solution Architecture document to define IAM@HHS component systems and services and align them to the HHS ICAM Segment Architecture and FICAM guidance.		$ 0.291

CMS Enterprise Identity Management – Digging Deeper

- **Business Case Available in pdf (web-scraper application?)**
- **USA Spending Contract Data**
- **Metrics & Performance Data**



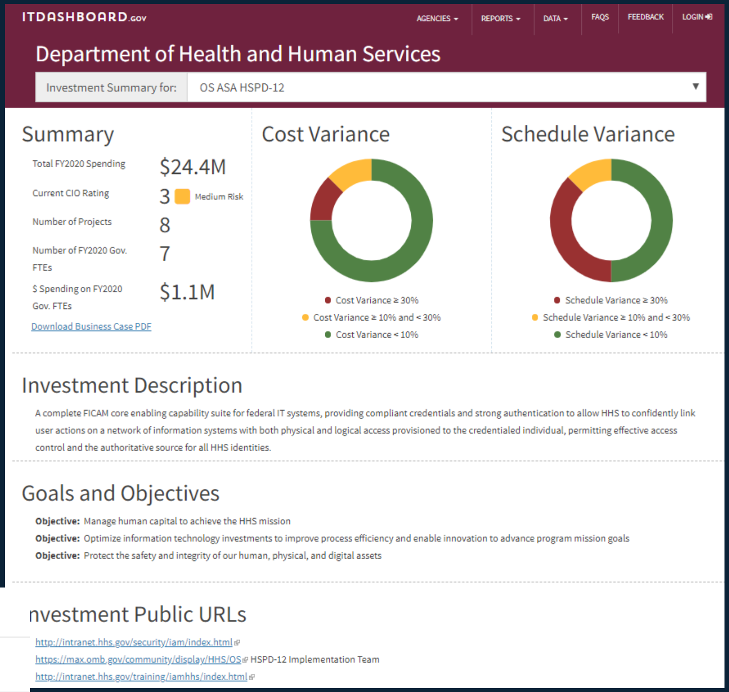
Business Case Detail **UII 009-000004093**

Business Case: Capital Asset Summary

Part I: Summary Information and Justification (All Capital Assets)

Section A: Overview & General Information

Date Investment First Submitted: 2011-09-16
Date of Last Change to Activities: 2017-09-14
Investment Auto Submission Date:
Date of Last Investment Detail Update: 2020-01-21
Date of Last Business Case Update: 2020-01-21
Date of Last Revision: 2020-01-21



Department of Health and Human Services

Investment Summary for: OS ASA HSPD-12

Summary

Total FY2020 Spending	$24.4M
Current CIO Rating	3 🟧 Medium Risk
Number of Projects	8
Number of FY2020 Gov. FTEs	7
$ Spending on FY2020 Gov. FTEs	$1.1M

Download Business Case PDF

Cost Variance

- ● Cost Variance ≥ 30%
- ● Cost Variance ≥ 10% and < 30%
- ● Cost Variance < 10%

Schedule Variance

- ● Schedule Variance ≥ 30%
- ● Schedule Variance ≥ 10% and < 30%
- ● Schedule Variance < 10%

Investment Description

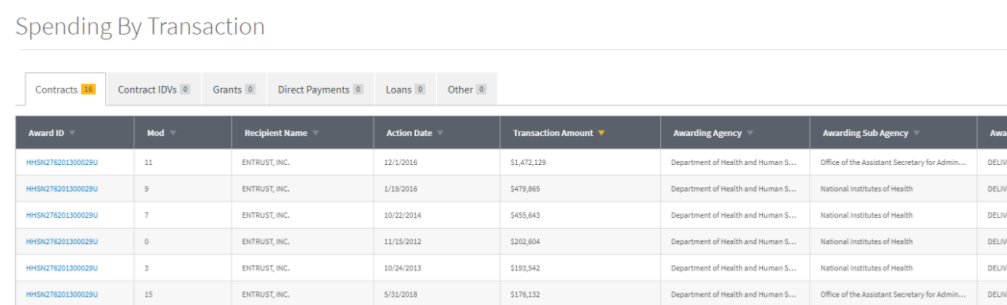
A complete FICAM core enabling capability suite for federal IT systems, providing compliant credentials and strong authentication to allow HHS to confidently link user actions on a network of information systems with both physical and logical access provisioned to the credentialed individual, permitting effective access control and the authoritative source for all HHS identities.

Goals and Objectives

Objective: Manage human capital to achieve the HHS mission
Objective: Optimize information technology investments to improve process efficiency and enable innovation to advance program mission goals
Objective: Protect the safety and integrity of our human, physical, and digital assets

nvestment Public URLs

http://intranet.hhs.gov/security/iam/index.html
https://max.omb.gov/community/display/HHS/OS HSPD-12 Implementation Team
http://intranet.hhs.gov/training/iamhhs/index.html

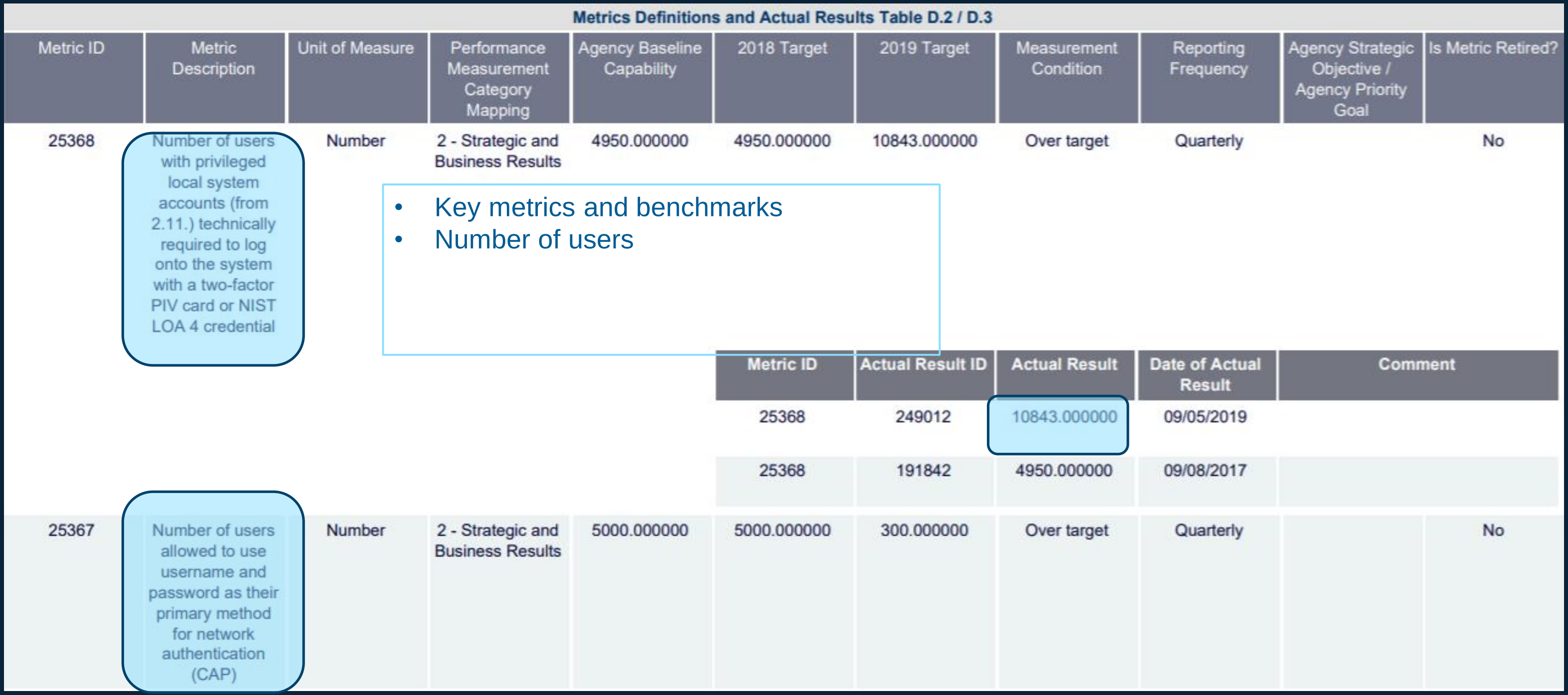


Spending By Transaction

Award ID	Mod	Recipient Name	Action Date	Transaction Amount	Awarding Agency	Awarding Sub Agency	Award Typ
HHSN276201300029U	11	ENTRUST, INC.	12/1/2016	$1,472,129	Department of Health and Human S...	Office of the Assistant Secretary for Admin...	DELIVERY
HHSN276201300029U	9	ENTRUST, INC.	1/19/2016	$479,865	Department of Health and Human S...	National Institutes of Health	DELIVERY
HHSN276201300029U	7	ENTRUST, INC.	10/22/2014	$455,643	Department of Health and Human S...	National Institutes of Health	DELIVERY
HHSN276201300029U	0	ENTRUST, INC.	11/15/2012	$202,604	Department of Health and Human S...	National Institutes of Health	DELIVERY
HHSN276201300029U	3	ENTRUST, INC.	10/24/2013	$193,542	Department of Health and Human S...	National Institutes of Health	DELIVERY
HHSN276201300029U	15	ENTRUST, INC.	5/31/2018	$176,132	Department of Health and Human S...	Office of the Assistant Secretary for Admin...	DELIVERY

CMS Enterprise Identity Management – Metrics/Users

- **Performance Data: what to measure and benchmarking**



Metrics Definitions and Actual Results Table D.2 / D.3

Metric ID	Metric Description	Unit of Measure	Performance Measurement Category Mapping	Agency Baseline Capability	2018 Target	2019 Target	Measurement Condition	Reporting Frequency	Agency Strategic Objective / Agency Priority Goal	Is Metric Retired?
25368	Number of users with privileged local system accounts (from 2.11.) technically required to log onto the system with a two-factor PIV card or NIST LOA 4 credential	Number	2 - Strategic and Business Results	4950.000000	4950.000000	10843.000000	Over target	Quarterly		No
25367	Number of users allowed to use username and password as their primary method for network authentication (CAP)	Number	2 - Strategic and Business Results	5000.000000	5000.000000	300.000000	Over target	Quarterly		No

Metric ID	Actual Result ID	Actual Result	Date of Actual Result	Comment
25368	249012	10843.000000	09/05/2019	
25368	191842	4950.000000	09/08/2017	

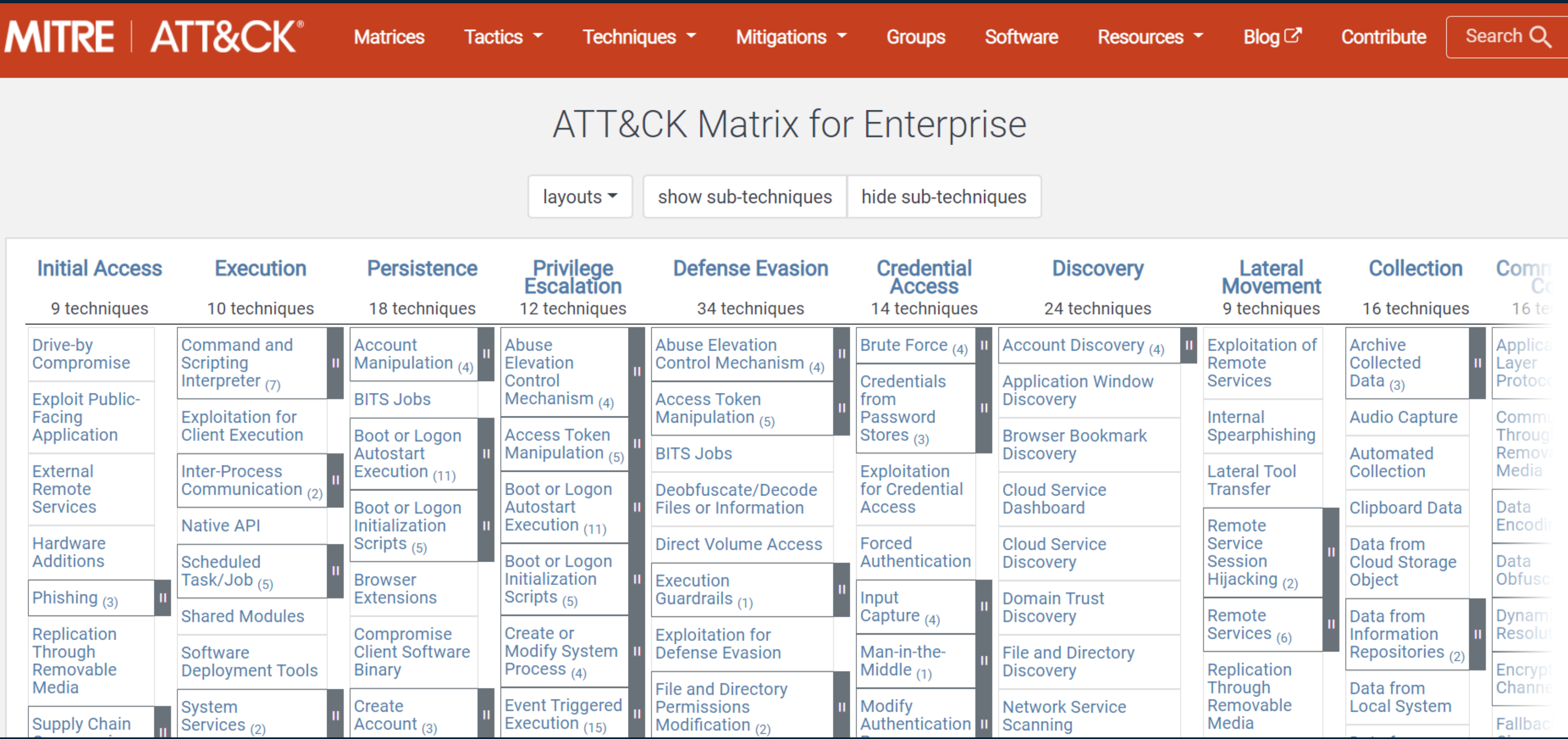
- Key metrics and benchmarks
- Number of users

Summary

1. **Cybersecurity costs are not well understood, but a lot can be learned by studying Federal IT System data reported via the public Office of Management and Budget (OMB) IT Dashboard**
   - Includes rich set of spending/budget data for cyber factors (but not CERs)
2. **Enough data to identify Benchmarks/Factors to use for estimating**
   - Cyber $ costs as % of Total Investment Program Expenditures
   - Cyber metrics
3. **Disparate data could be mapped into “Cyber Cost Categories” to establish factors by logical groupings**
4. **Cyber costs included 5 categories consistently; roughly a dozen others as “spikes”**

Future Ideas…

MITRE | ATT&CK®



ATT&CK Matrix for Enterprise

Initial Access — 9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain

Execution — 10 techniques

- Command and Scripting Interpreter (7)
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services (2)

Persistence — 18 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (11)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)

Privilege Escalation — 12 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (11)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Event Triggered Execution (15)

Defense Evasion — 34 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)

Credential Access — 14 techniques

- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (4)
- Man-in-the-Middle (1)
- Modify Authentication

Discovery — 24 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning

Lateral Movement — 9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media

Collection — 16 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Information Repositories (2)
- Data from Local System

Comm C — 16 te

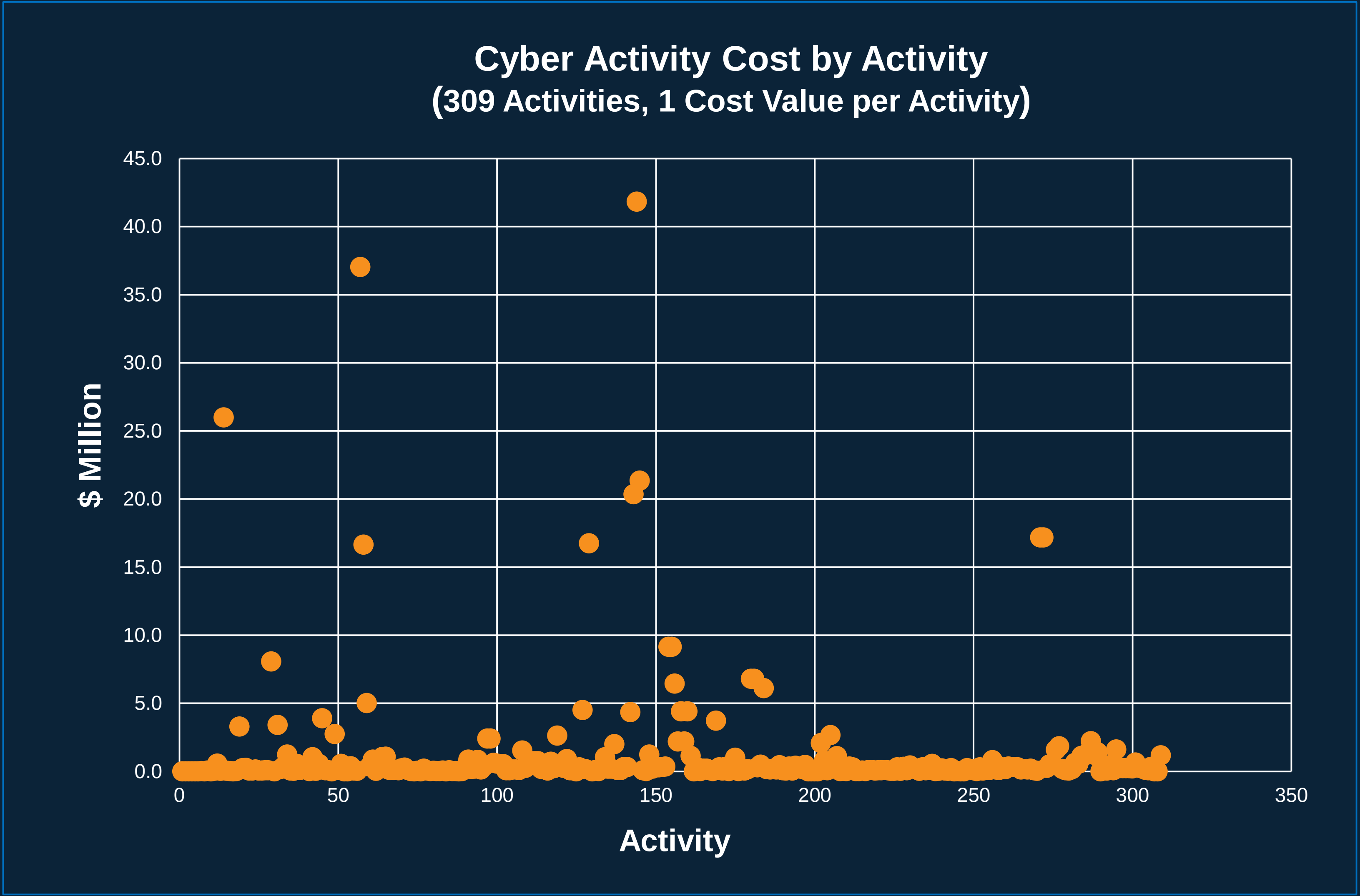
- Applica Layer Protoc
- Comm Throug Remov Media
- Data Encodi
- Data Obfusc
- Dynam Resolu
- Encryp Channe
- Fallbac

Glossary of Additional Acronyms

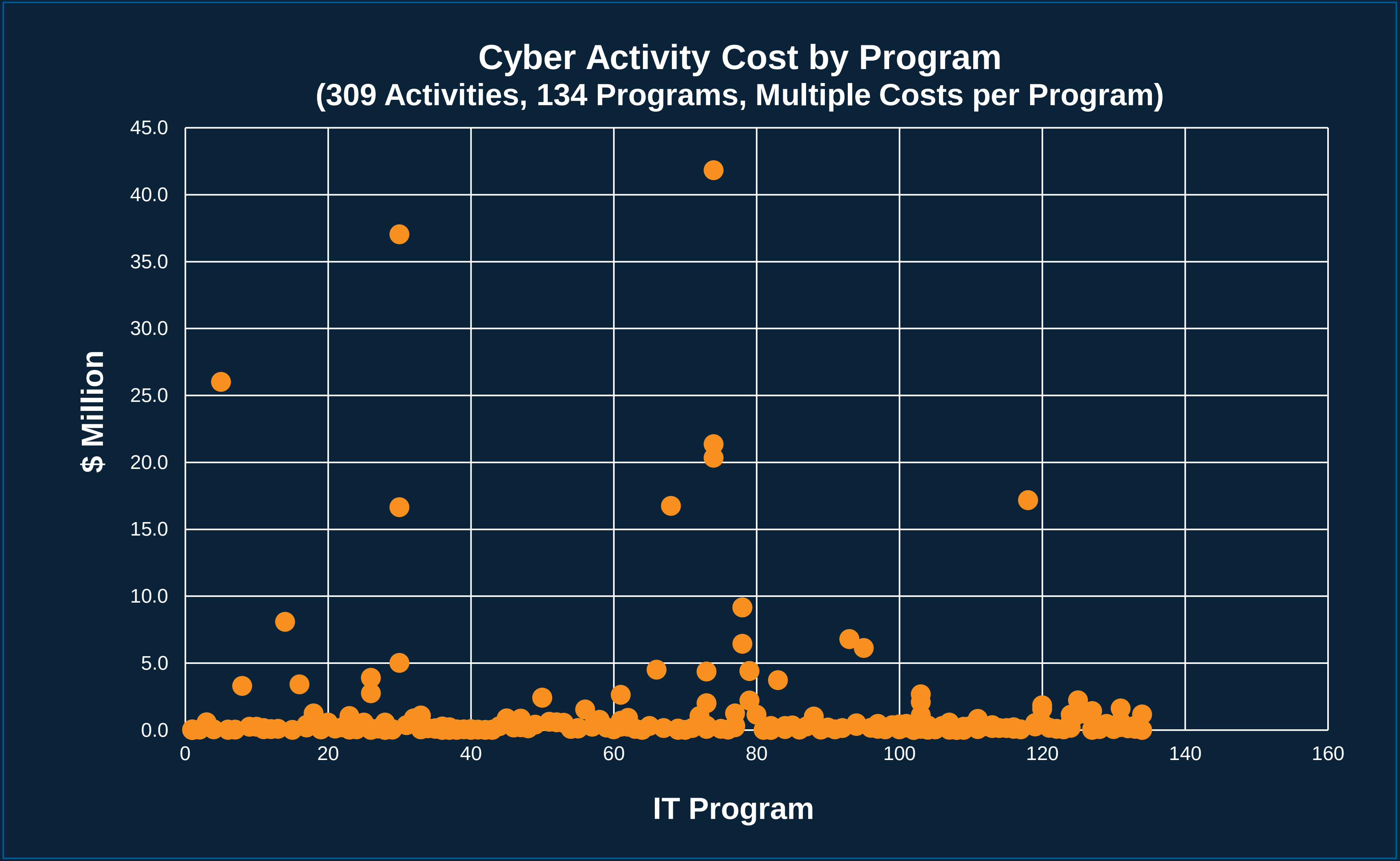
Acronym	Definition
DoI	Department Of Interior
DoJ	Department Of Justice
HHS	Health And Human Services
IAVA	Information Assurance Vulnerability Alert
ICAM	Identity Credential Access Management
NIST	National Institute Of Standards and Technology
OpDiv	Operational Division
PIV	Personal Identity Verification
PMO	Program Management Office
WBS	Work Breakdown Structure

Back-Up Slides

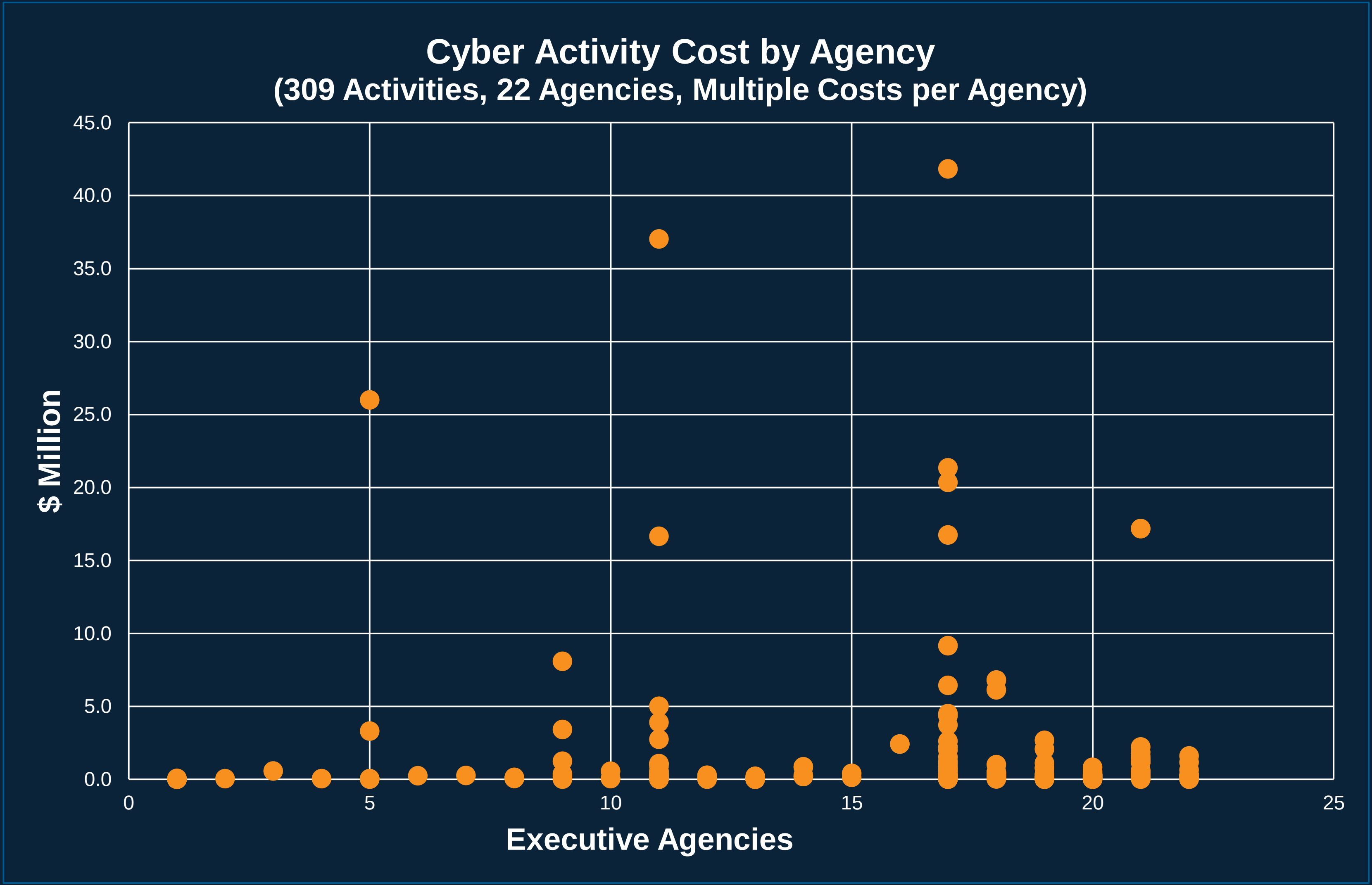
Data Presentation



Data Presentation



Data Presentation


Cyber Activity Cost by Agency
(309 Activities, 22 Agencies, Multiple Costs per Agency)
$ Million
Executive Agencies