



U.S. General Services Administration

# Highly Adaptive Cybersecurity Services (HACS) Workshop

Shon Lyublanovits

6/13/2016



- Background
- Cybersecurity Services RFI Overview
- Cybersecurity Services RFI Analysis
- Next Steps
- Questions



As a result of the President’s request for a Cybersecurity National Action Plan (CNAP) and OMB’s Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, GSA was directed to research contract vehicle options and develop a capability to deploy incident response services that can quickly be leveraged by Federal agencies.

## Approach

GSA SME’s are working with DHS and OMB to develop the CSIP/CNAP solution:

- Provided an Implementation Plan to OMB regarding contract vehicle options in response to CSIP
- Conducted market research and provided a list of vendors to OMB who are capable of providing some or all of the Proactive, Reactive, and Remediation capabilities
- Developed requirements for Proactive, Reactive, and Remediation capabilities
- Updated Cybersecurity Web Page
  - Created Buy/Sell Cybersecurity Products and Services pages
  - Posted Ordering Procedures and Proactive Risk and Vulnerability Assessment (RVA) Statement of Work (SOW) Templates
- Developed “CSIP Contract Vehicle Options” and posted on Acquisition Gateway IT Security Hallway
- Issued the Cybersecurity Services RFI on April 11, 2016 to inquire about current offerings in the Proactive Services, Reactive Services, and Remediation Services categories



# Cybersecurity Services RFI Overview

## Request for Information (RFI)

- Released April 11, 2016
- Closed April 20, 2016
- Requested input on 12 capabilities (Proactive, Reactive and Remediation)

## RFI Goals

- Gain feedback from industry and any other relevant stakeholders dealing with Cybersecurity
- Better understand how industry partners are selling cybersecurity services today on IT Schedule 70

## RFI Responses

- 122 vendors provided feedback, 119 met the RFI requirement:
  - On Schedule 70 - 70
    - Small Business - 36
    - Large Business - 34
  - Vendors Sold Through Resellers - 9
  - Not on Schedule 70 - 49



# Cybersecurity Services RFI Analysis

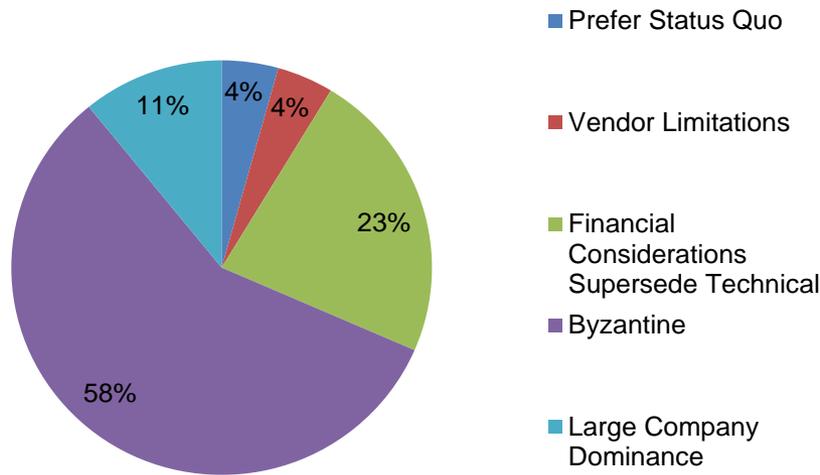
- Suggested additions to cybersecurity services offerings - Sample

| <b>Additional Recommended Services</b> | <b>Number of Suggestions</b> |
|--|------------------------------|
| Digital Forensics (Network and Host)   | 13                           |
| Secure Code Analysis                   | 6                            |
| Demonstrations                         | 6                            |
| Cyber Risk Management                  | 4                            |
| Endpoint Security                      | 12                           |
| Cyber Threat Intelligence              | 16                           |
| SCADA Risk Management                  | 12                           |
| Next Generation                        | 10                           |
| Advanced Threat Protection (ATP)       | 5                            |

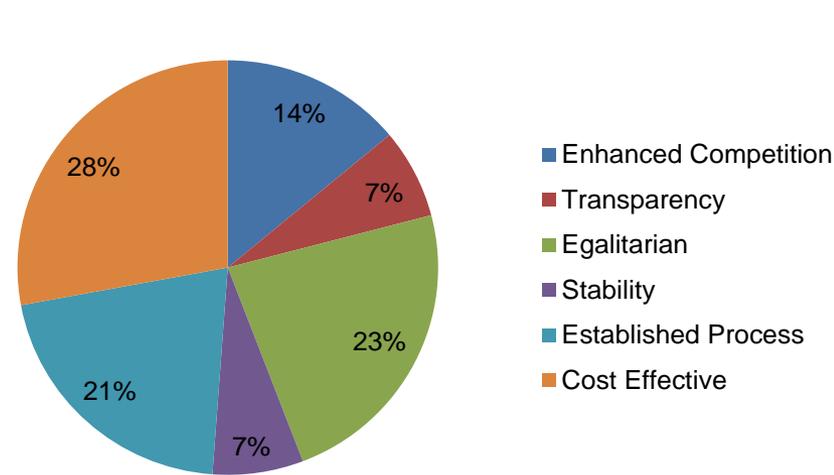
# Cybersecurity Services RFI Analysis

*What are the advantages and/or disadvantages of how the government currently purchases cybersecurity products and services?*

## Disadvantages



## Advantages



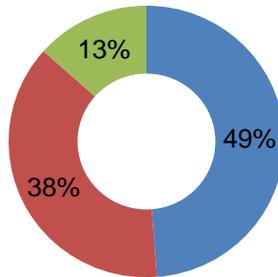
- Most respondents expressed dismay over what they determined to be the “byzantine” nature of the government procurement process. The “length,” “complication,” and “limitations” inherent in government contracting are an impediment to the necessarily rapid deployment of cybersecurity services.
- About a quarter of respondents conceive that the current vehicles allow the government to acquire products at marked discounts, due to volume pricing and versatility of the vehicles in question.

# Cybersecurity Services RFI Analysis

*What contracting type and pricing methodology structures are currently and/or should be offered for the government to purchase proposed cybersecurity service(s)?*

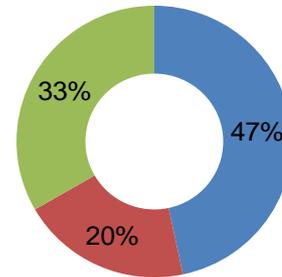
## Preferred Contract Types

■ FFP/FFP-LOE ■ T&M ■ CPFF



## Preferred Contract Vehicles

■ IDIQ ■ GWAC ■ BPA

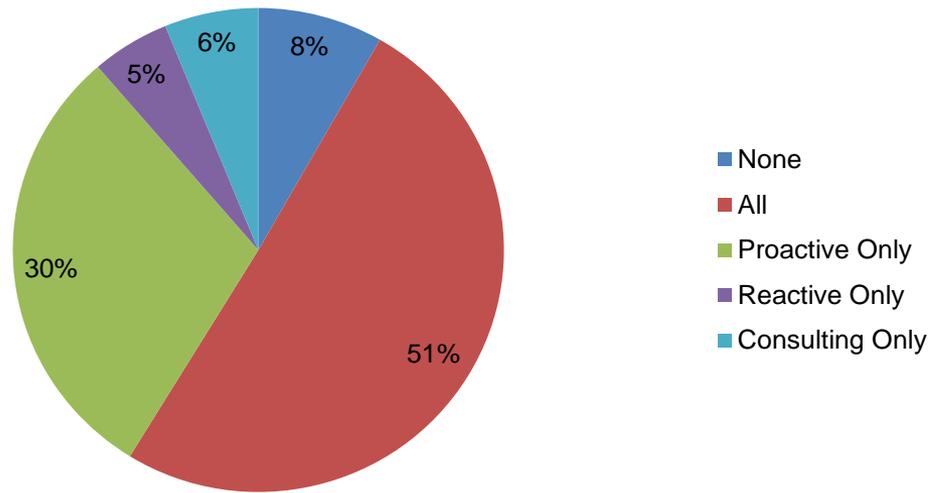


- Most respondents were knowledgeable about the standard contract types awarded in both the public and private sector, with the Firm Fixed Price (FFP) and Time and Material (T&M) being chief among them.
- Those businesses that claim a variety of government sourced contracts usually route such transactions through a wide range of vehicles, including the GSA Schedules (IT 70, OASIS, Alliant), the CIO-SP3, the DHS EAGLE II, ITES-2S, and NASA-SEWP.

# Cybersecurity Services RFI Analysis

*What types of cybersecurity products and services are most commonly sold to your private sector customers?*

## Services Offered to the Private Sector

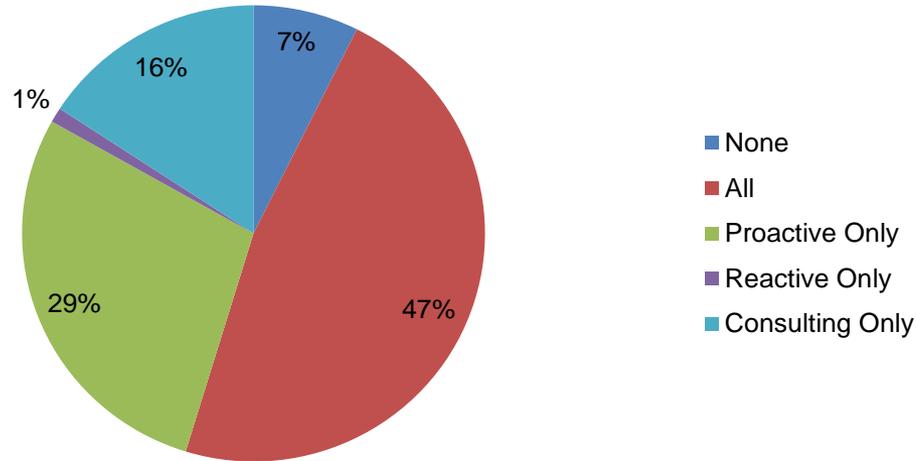


- Slightly more than half of all respondents offer both proactive and reactive services to private sector customers, though some specialize in addressing threats of a particular nature, whether they are Distributed Denial of Service (DDoS) attacks, Advanced Persistent Threats (APT)s, or a form of information leakage.

# Cybersecurity Services RFI Analysis

*What types of cybersecurity products and services are most commonly sold to your Government customers?*

## Services Offered to the Public Sector

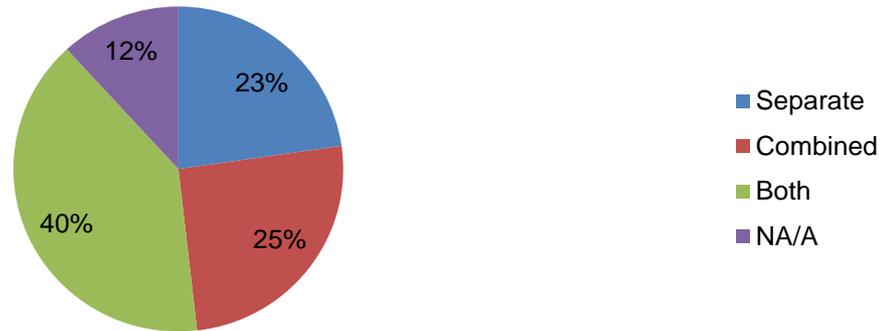


- All or a combination of proactive and reactive cybersecurity services are offered to governmental agencies by nearly half of the RFI respondents.
- The proactive services most commonly offered were vulnerability scanning and penetration testing while reactive services usually included incident response and security engineering/remediation.

# Cybersecurity Services RFI Analysis

*Are the cybersecurity services listed in Section B. generally procured separately or combined by industry and/or the government?*

## Procurement Trend of Cybersecurity Services

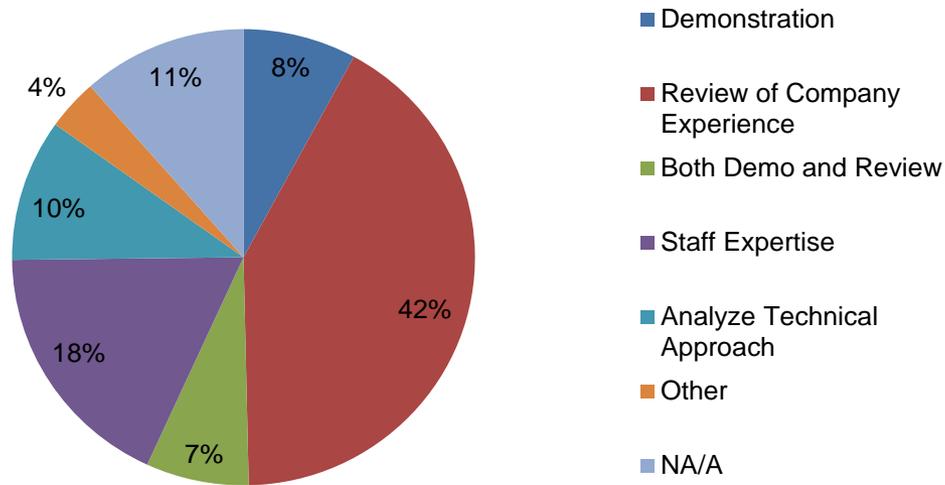


- A plurality of firms asserted that services were offered in a customized fashion, either *a la carte* or in “bundles,” to suit the needs of the client. This versatile offering is an attempt to accommodate companies and agencies that are disparate in size, resources, and IT architecture.
- General response trends suggest that of all Section B services, penetration testing should both be unbundled and third party provided. This ensures the team tasked with penetration testing is completely unfamiliar with the system being tested, enabling insights that may be missed in a routine vulnerability assessment.

# Cybersecurity Services RFI Analysis

*How should the government evaluate the ability of an offeror to provide the cybersecurity services listed in Section B.?*

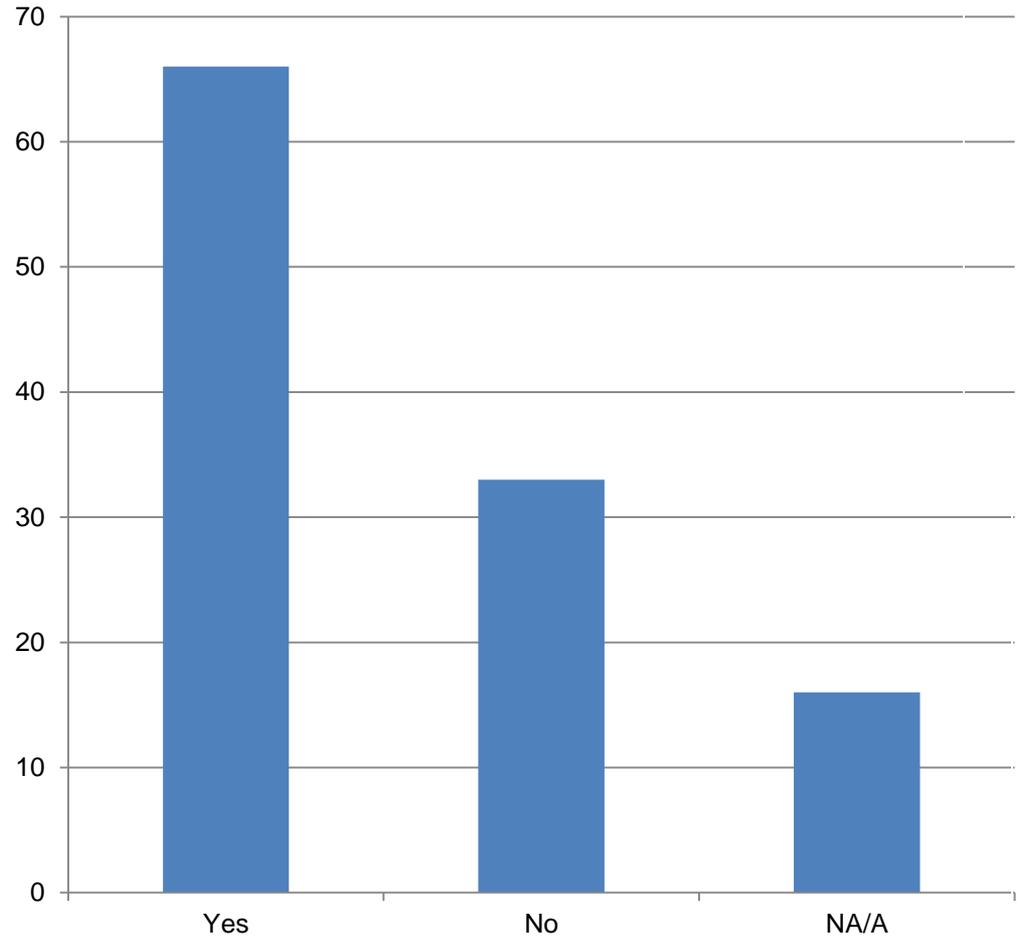
## Evaluation Suggestions



- A sizeable percentage of respondents prefer a review of the candidate’s past performance in both the private and public sector.
- They also recommend use of existing survey programs like the Contractor Performance Assessment Reporting System (CPARS) and client reviews to render a “best value” assessment of any proposal.

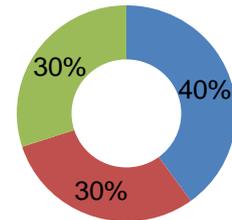
# Cybersecurity Services RFI Analysis

*Should the government require or provide positive weight to offerors that have certain certifications or credentials in some or all of the cybersecurity services listed in Section B? Which and in what way?*



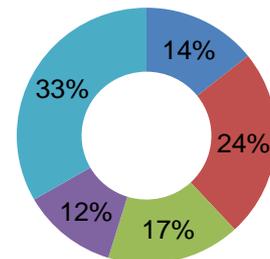
## Preferred Accreditation Bodies

ISO/IEC CMMI CIRA



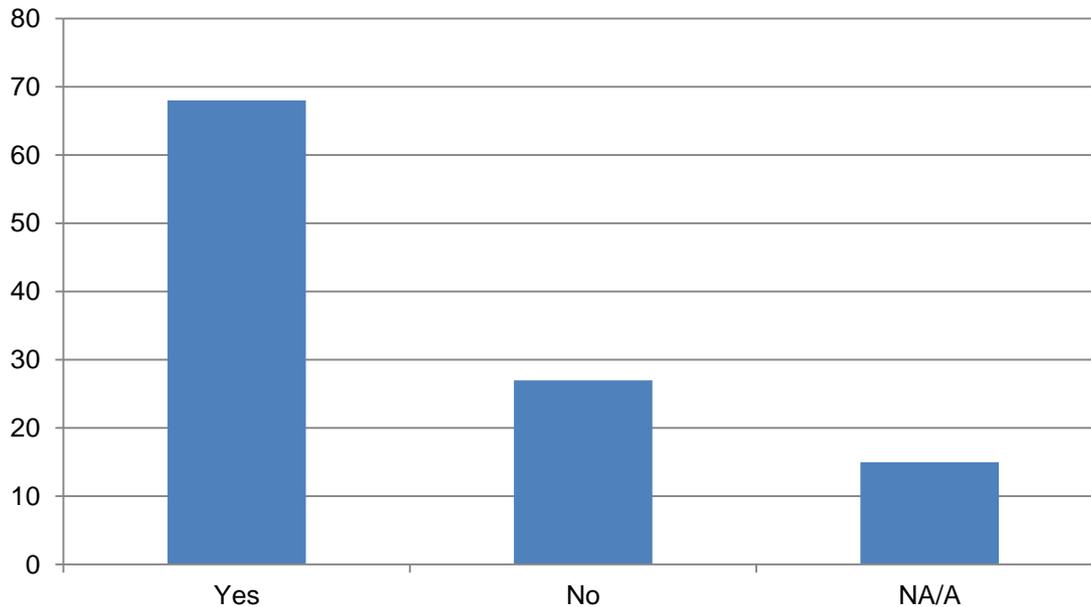
## Preferred Individual Certs

CompTIA suite (ISC)2 suite ISACA suite SANS suite CEH



# Cybersecurity Services RFI Analysis

*Should the government consider the use of demonstration projects (e.g., “capture the flag”) in evaluating an offeror’s ability in some or all of the cybersecurity services listed in Section B? What type of demonstration and for which services?*

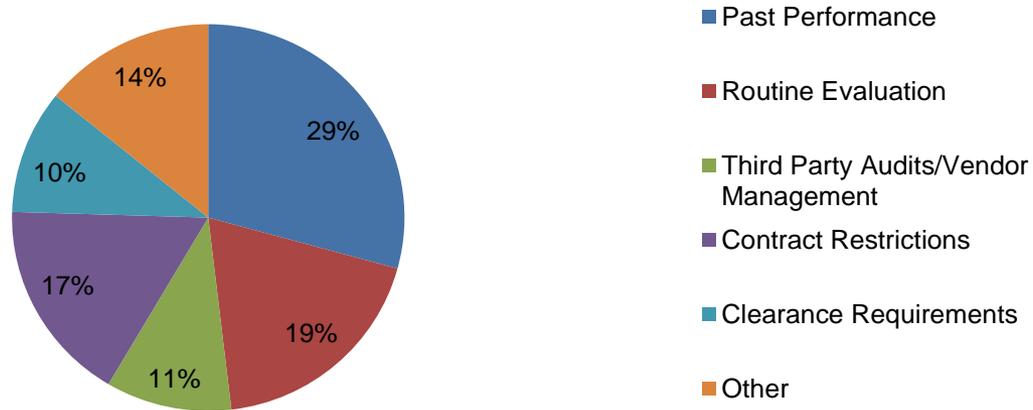


- The vast majority of respondents support the use of demonstrations as a means to accurately reflect what talent and technology they offer. This provides an avenue for innovative yet obscure products to be brought to the fore, and for enormous talent to be recognized from companies both large and small.

# Cybersecurity Services RFI Analysis

*How should the government ensure the fidelity and responsibility of contractors who provide cybersecurity products?*

## Fidelity and Responsibility Suggestions



- As evidenced above, more than a quarter of respondents contend that a review of past performance should be a central element in determining the reliability of contractors. CPARS is believed to be an excellent source of knowledge in that regard.
- A large amount of respondents attest that stringent contractual requirements are sufficient in enforcing vendor compliance, with severe penalties should any terms be violated.

# Cybersecurity Services RFI Analysis

*How can we ensure that the government can access cybersecurity resources and services as quickly as possible when necessary?*

- There is near unanimous clamoring for a new, cybersecurity specific purchasing vehicle or leveraging of existing ones to accommodate these products and services.
  - Whether it is in the form of a new Blanket Purchase Agreement (BPA), Government-wide Acquisition Contracts (GWAC), Special Item Number (SIN), or some other iteration of an IDIQ award.
  - Vendors want immediate access to any rapid acquisition agreement and for the government to maintain a list of pre-approved cybersecurity providers.
  - Sole source task orders and Request for Proposal (RFP) templates were also suggested to reinforce the government's current array of contract schemes.
- Other suggested ideas include maintaining reserve cybersecurity staff, devising surge capacity process for reinforcement of staff, and shifting to cloud-based services.

- Host Cybersecurity Services Workshop (Industry and Government) (6/13/2016)
- Release second RFI (Cybersecurity SIN) (6/8/2016 - 6/21/2016)
- Analyze second RFI Responses (6/24/2016)
- Publish RFI Results (6/27/2016)
- Draft Cybersecurity SIN Business Case (6/14/2016 - 7/21/2016)
- Create Cybersecurity Services SIN (9/13/2016 - 9/30/2016)

---

**Questions?**