Virginia Cybersecurity Planning Committee
October 18, 2023 – 10am
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson, Chair Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Grant Update	Robbie Coates, Director, Grant Management and Recovery Division, Va Department of Emergency Management
Survey of Interest	Mike Watson
Contract Options Discussion	
Prioritizing Year 1 Funds Discussion (Priorities, Process, etc.)	
Public Comment Period	
Other Business	Staff
Adjourn	

Virginia Cybersecurity Planning Committee
August 16, 2023, 10am
7325 Beaufont Springs Dr, Mary Jackson Boardroom
Richmond, VA, 23225

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10am. Mr. Watson welcomed the members.

Presiding:

Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present:

Diane Carnohan, Chief Information Security Officer, Virginia Department of Education

Adrian Compton, Tribal Administrator, Monacan Indian Nation

Charles DeKeyser, Major, Virginia Army National Guard. Major Dekeyser is on temporary duty from his home base for the National Guard.

Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems

Maj. Eric W. Gowin, Division Commander- Information Technology Division, Virginia State Police. Mr. Gowin participated virtually due to work reasons.

John Harrison, IT Director, Franklin County

Derek M. Kestner, Information Security Officer, Supreme Court of Virginia

Benjamin Shumaker, Cyber Security Specialist, King William County Government

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice

Stephanie Williams-Hayes, Chief Information Security Officer, Virginia Department of Health

Members Participating Remotely:

Michael Dent, Chief Information Security Officer, Fairfax County Department of Information Technology

Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Mr. Dent and Mr. Williams participated remotely because their principal residence is more than 60 miles away.

Members Not Present:

Aliscia N. Andrews, Deputy Secretary of Homeland Security, Office of the Governor

Robbie Coates, Director, Grant Management and Recovery, VDEM

Staff Present:

Leslie Allen, Senior Assistant Attorney General, Office of the Attorney General

Joshua Heslinga, Director of Legal & Legislative Services, Virginia IT Agency

Catherine Lee, Preparedness Grants Manager, Virginia Department of Emergency Management

Mylam Ly, Legal Compliance & Policy Specialist, Virginia IT Agency

Chelsea Oppong, Intern, Virginia IT Agency

Trey Stevens, Deputy Chief Information Security Officer, Virginia IT Agency

Review of Agenda:

Ms. Ly provided an overview of the agenda and corresponding items in the digital meeting packets.

Approval of Minutes:

The June meeting minutes were displayed on the screen. Major Gowin offered an amendment to the meeting minutes, Major Dekeyser and Major Gowin were present for the June meeting. Upon a motion by Major Gowin and duly seconded by Major Dekeyser, the committee unanimously voted to adopt the amended meeting minutes.

Updates

The Virginia Department of Emergency Management (VDEM) has taken steps to send the plan to both CISA (Cybersecurity and Infrastructure Security Agency) and FEMA (Federal Emergency Management Agency). Additionally, it was mentioned Year 2 of the Notice of Funding Opportunity (NOFO) was released. There is no needed action from the committee currently.

Communications Plan

Ms. Legrand presented an update to the communications plan, beginning with background information and the provision of crucial resources. She outlines the communications that have already been distributed to targeted audiences, including education stakeholders, local government, including VACo, VML, VaLGITE and VDEM. The VACo newsletter is scheduled for release on the 25th, providing an additional avenue for reaching a broader audience. Ms. Legrand highlighted the importance of ensuring that all relevant entities, including schools are captured in the communications. In addition to the mentioned recipients, VACorp and VRSA were identified as additional parties to receive these communications. A new listserv was established specifically for this grant opportunity with 167 subscribers. The communications plan is structured into phases. With Phase 2 focusing on ongoing information sharing and Phase 3 on notifying recipients of grant awards. The presentation concluded with an opportunity for questions.

Draft Survey

Feedback and suggestions for improving the draft survey were discussed. The discussion focused on several key areas. There was a call to clarify the survey objectives to ensure their relevance and importance were clearly understood. Confidentiality language was a point of concern. The discussion revolved around safeguarding the cybersecurity posture of organizations without putting localities at risk. To address these concerns, it was suggested that language similar to the Freedom of Information Act (FOIA) be incorporated into the survey to provide a framework for confidentiality. Various possibilities for maintaining confidentiality were explored. These included relying on existing provisions of law, reporting aggregate data rather than individual responses, and assuring respondents their survey information would be protected. A practical suggestion was made to prioritize the last question by moving it to the beginning of the survey, ensuring respondents are aware of its significance. The survey should include language that assures the respondents they will not face penalties for providing pre-existing contract information. To avoid ambiguity, it was recommended that objective 1.2 be better defined to provide clarity to respondents. Instructions should be included to guide respondents on what to do when they don't understand the context of a question. On objective 1.3, concerning third-party assistance, should be further clarified, and explained to avoid any potential misunderstandings. A notable discussion point was the use of .gov domains for schools, particularly K-12 schools. To ensure consistency and security, there was a suggestion for Department of Education to create standards for K-12 schools to transition to .gov domains. Categorization of schools, such as school locality and elections were proposed along with the inclusion of parentheses for all acronyms enhancing clarity. Consideration was given to include a question for vendors who may be filling out the survey on behalf of localities. It was recommended to specify the estimated time needed to complete the survey and offer a progress meter.

Break

The committee took a 5-minute break

Public Comment Period:
Carl Dodson – Regional SOC in the town of Culpeper. Spoke on collection of SOCs to support all localities.

Other Business:
Mr. Watson opened the floor for other business. The next meeting is September 20 at 10am and discussed travel documents. There were questions raised concerning legislation, although it was clarified that legislative matters would not be able to be discussed during the meeting.

There was a request for a document outlining the Freedom of Information Act (FOIA) exemptions to be provided at the next meeting. The intention behind the request is to offer a more general summary of FOIA exemptions for the benefit of the committee.

Adjourn
Upon a motion by Mr. Kestner and duly seconded by Major DeKeyser, the committee unanimously voted to adjourn the meeting at 11:35am.

VIRGINIA
IT AGENCY

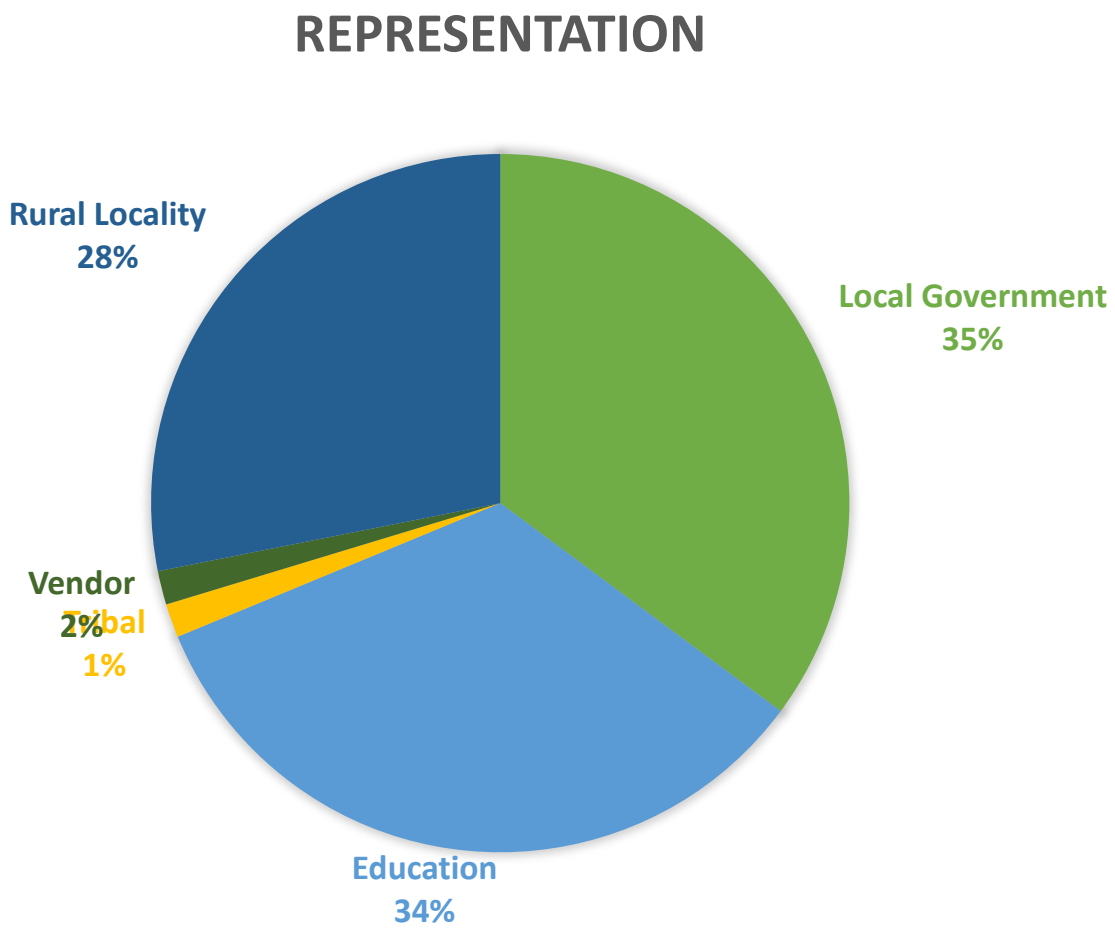
Results from the Survey of Interest

Michael Watson, Chair
Chief Information Security Officer of the Commonwealth

Oct. 18, 2023

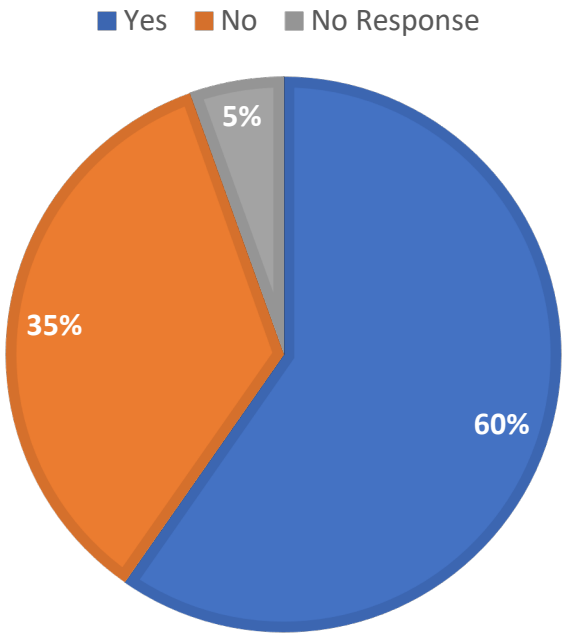
Summary

- 140 applicants
- Removed 9 entries that were incomplete or non-valid entries “xxx”



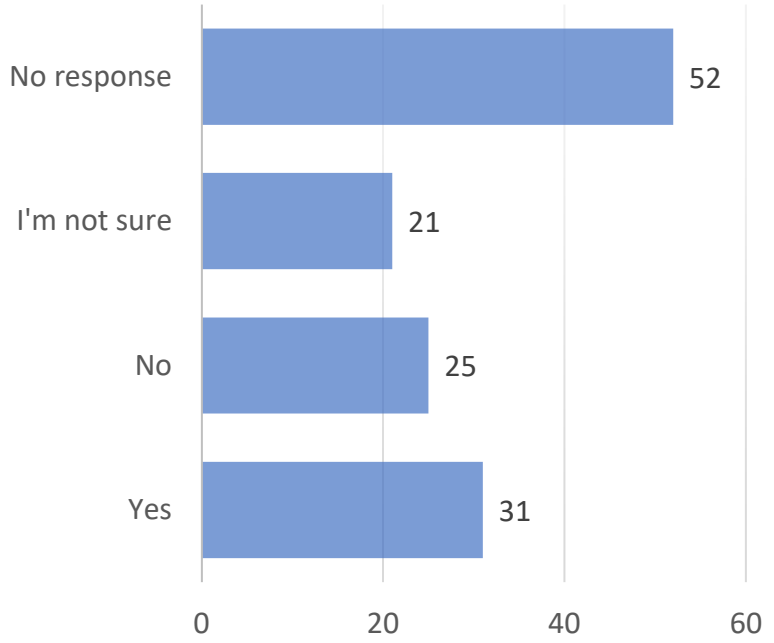
Objective 5.1 - Identify security gaps associated with program objectives which can be supported by the grant program
Objective 5.3 - Network and system architecture diagram and assessment

For these objectives, do you need a third party to perform a review of your environment and put together a roadmap for using the grant?



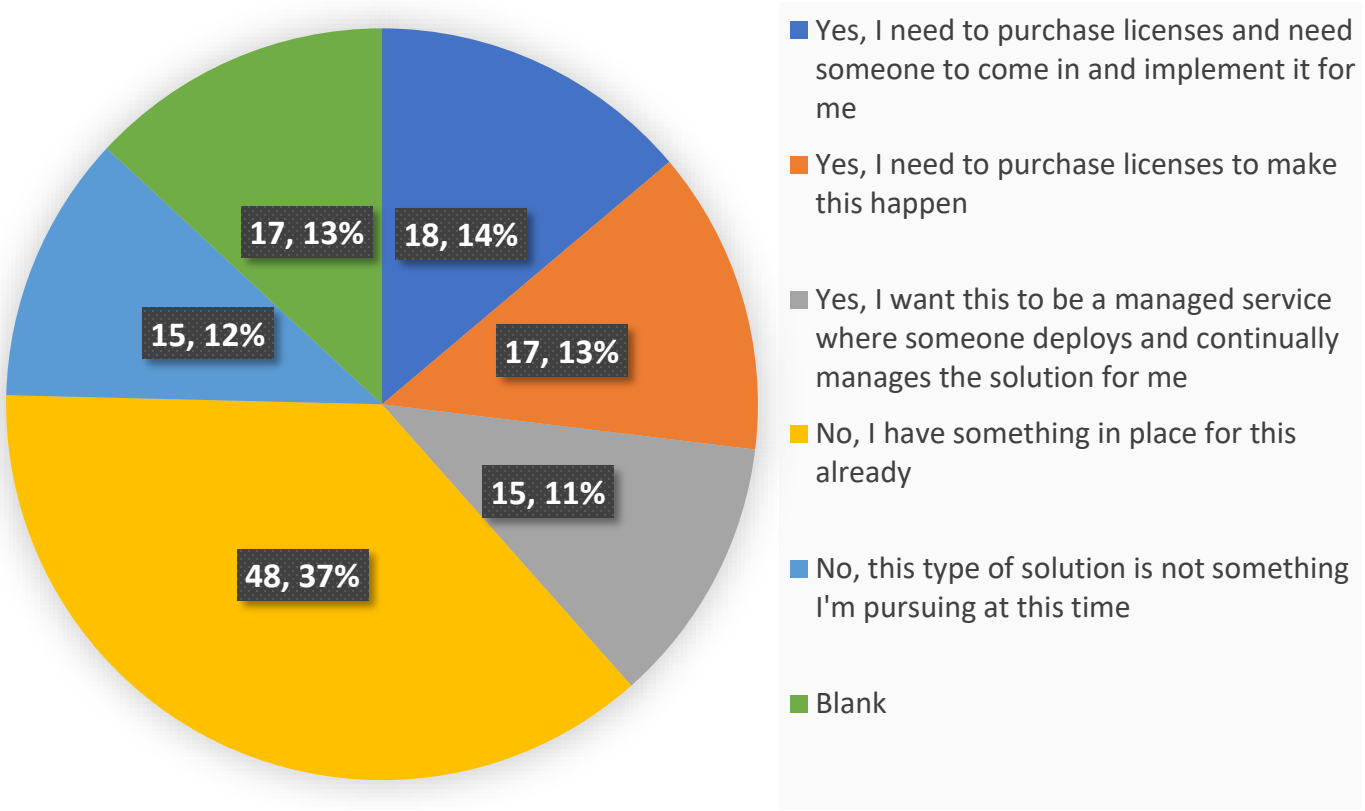
25 out of 77 “yes” respondents, or approximately 33% were from rural localities

Do you also need a third party to provide a network and system architecture diagram?

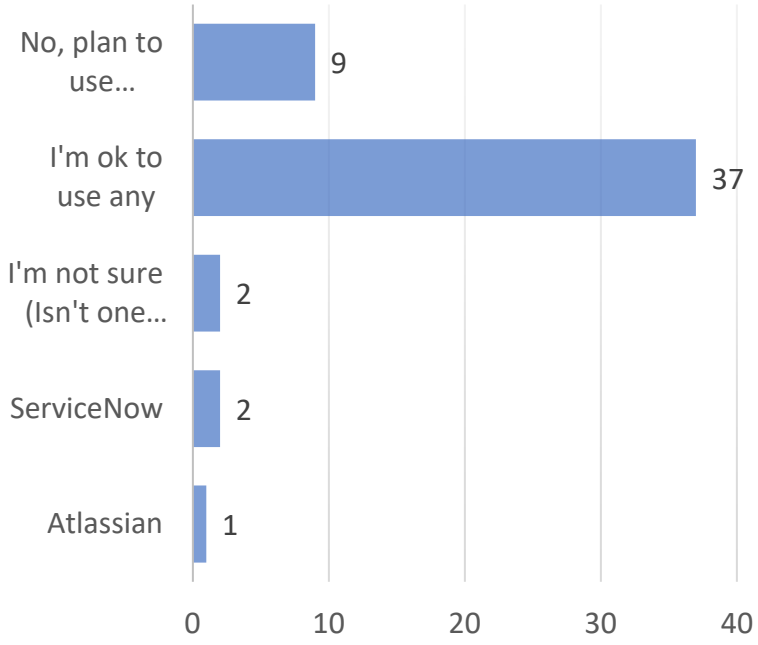


Objective 1.1 - Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software)

For this objective, are you looking for a solution for tracking hardware and software?

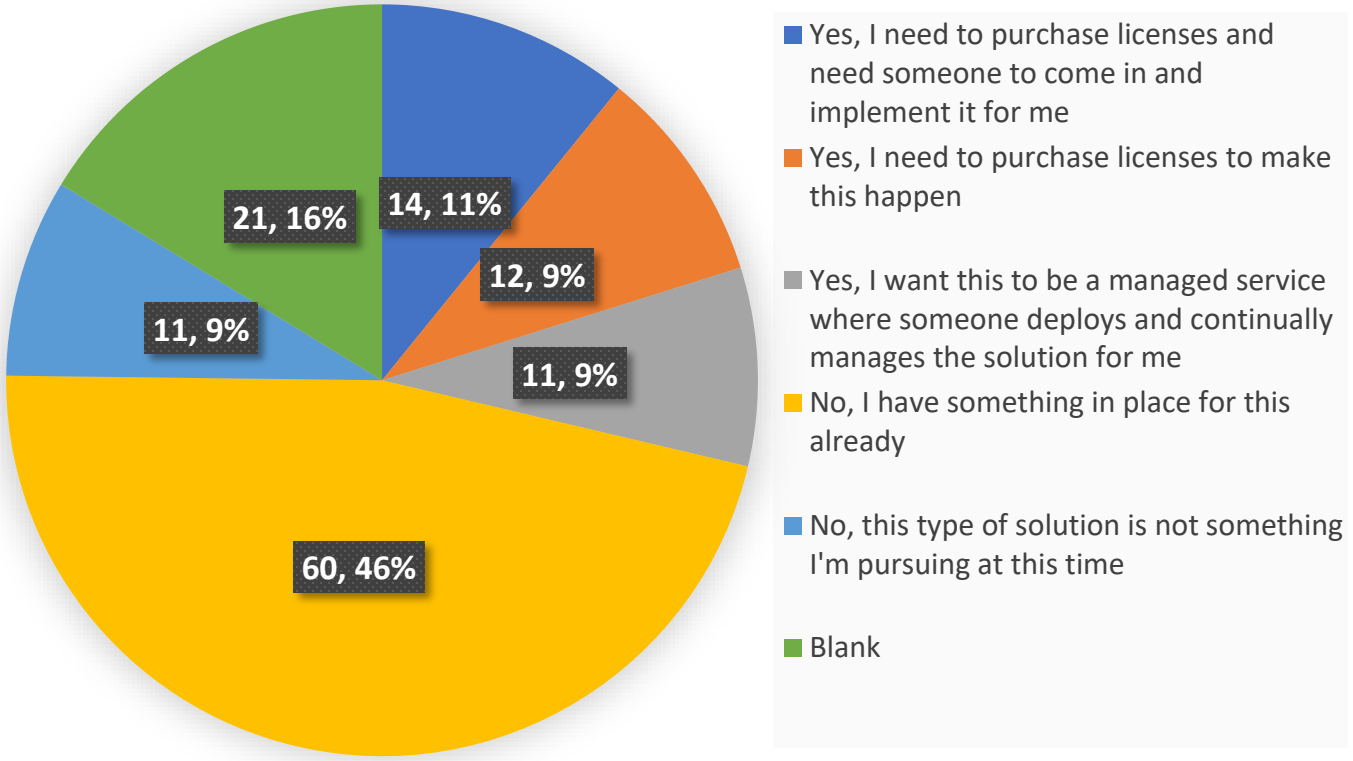


Would you plan to use any of the following software and/or services for this solution?

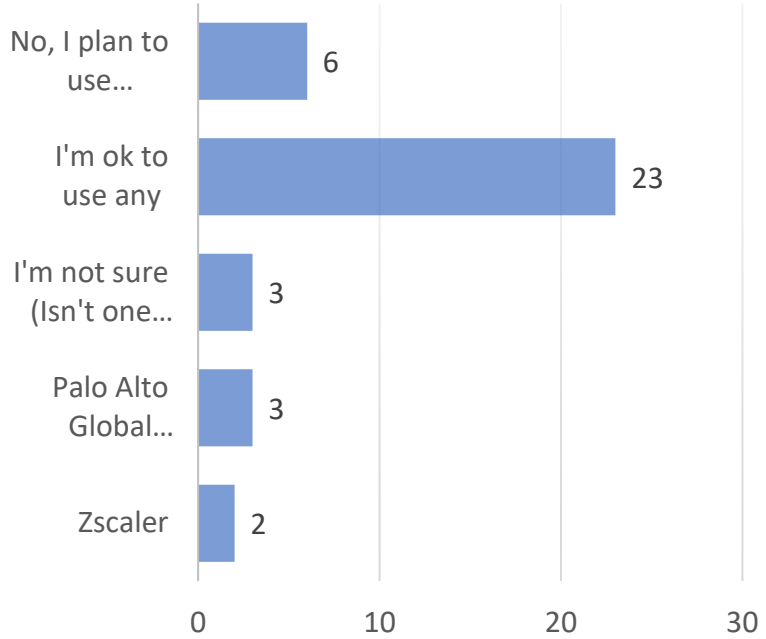


Objective 1.2 - Ensure only authorized assets connect to enterprise systems and are inventoried

For this objective, are you looking for a virtual private network (VPN) or zero trust network access solution?

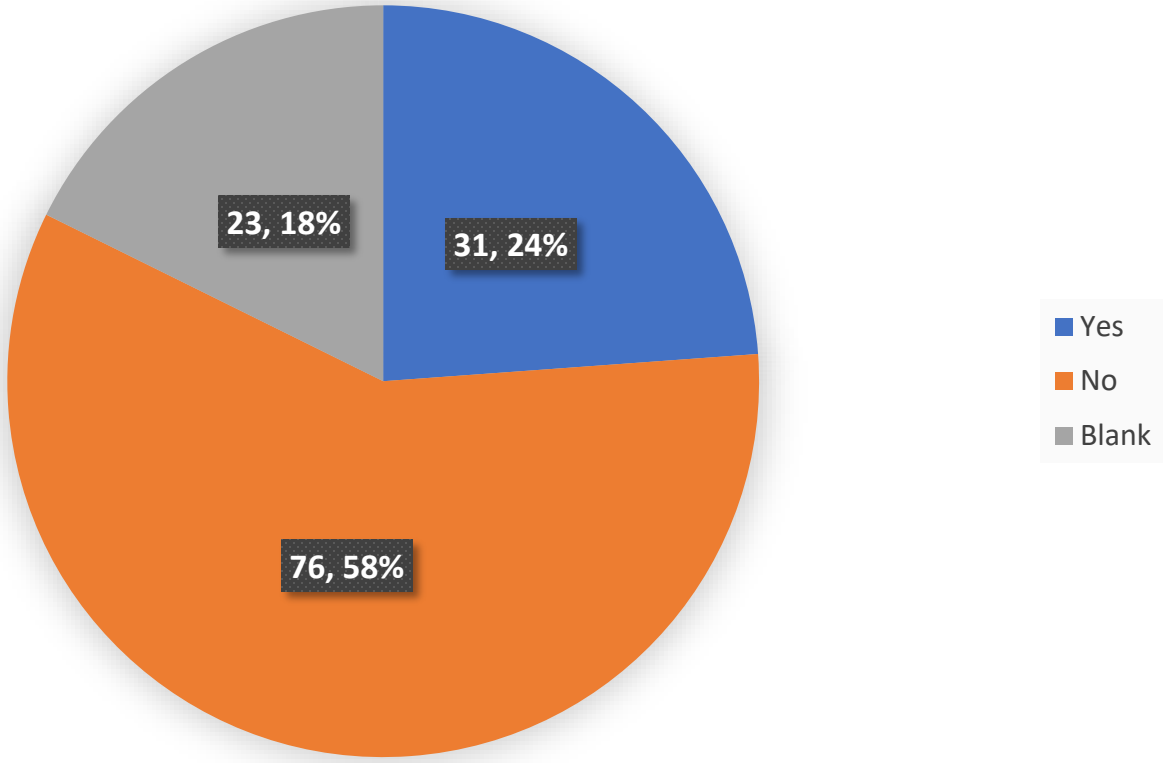


Would you plan to use any of the following software and/or services for this solution?



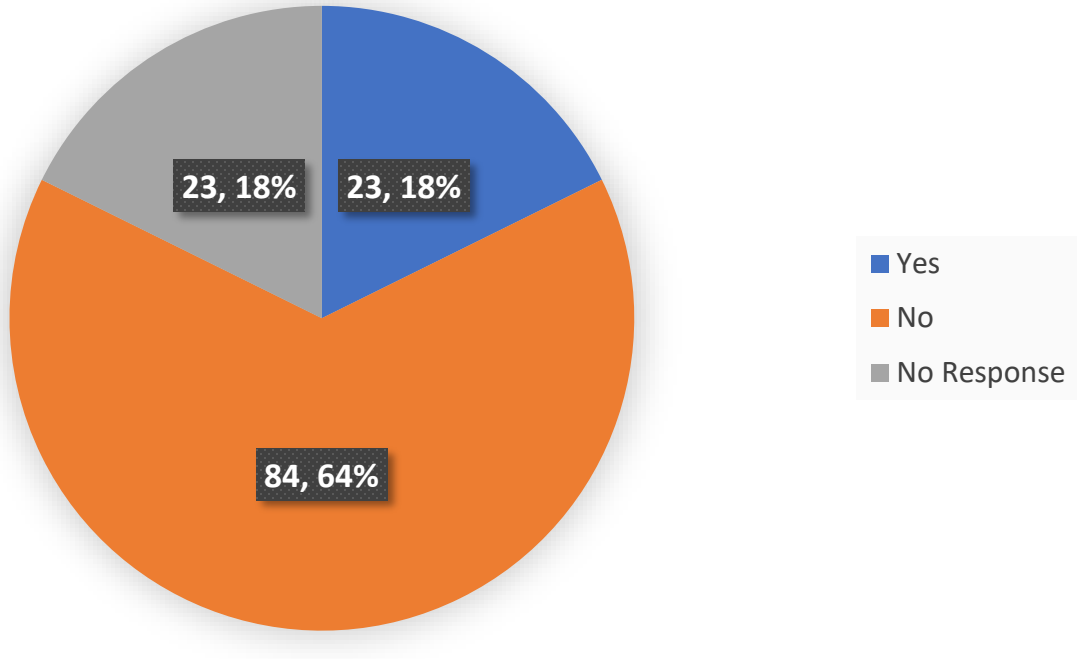
Objective 1.3 - Upgrade or replace all software no longer receiving security maintenance/support

For this objective, do you need third-party assistance to upgrade a system no longer receiving security patches?



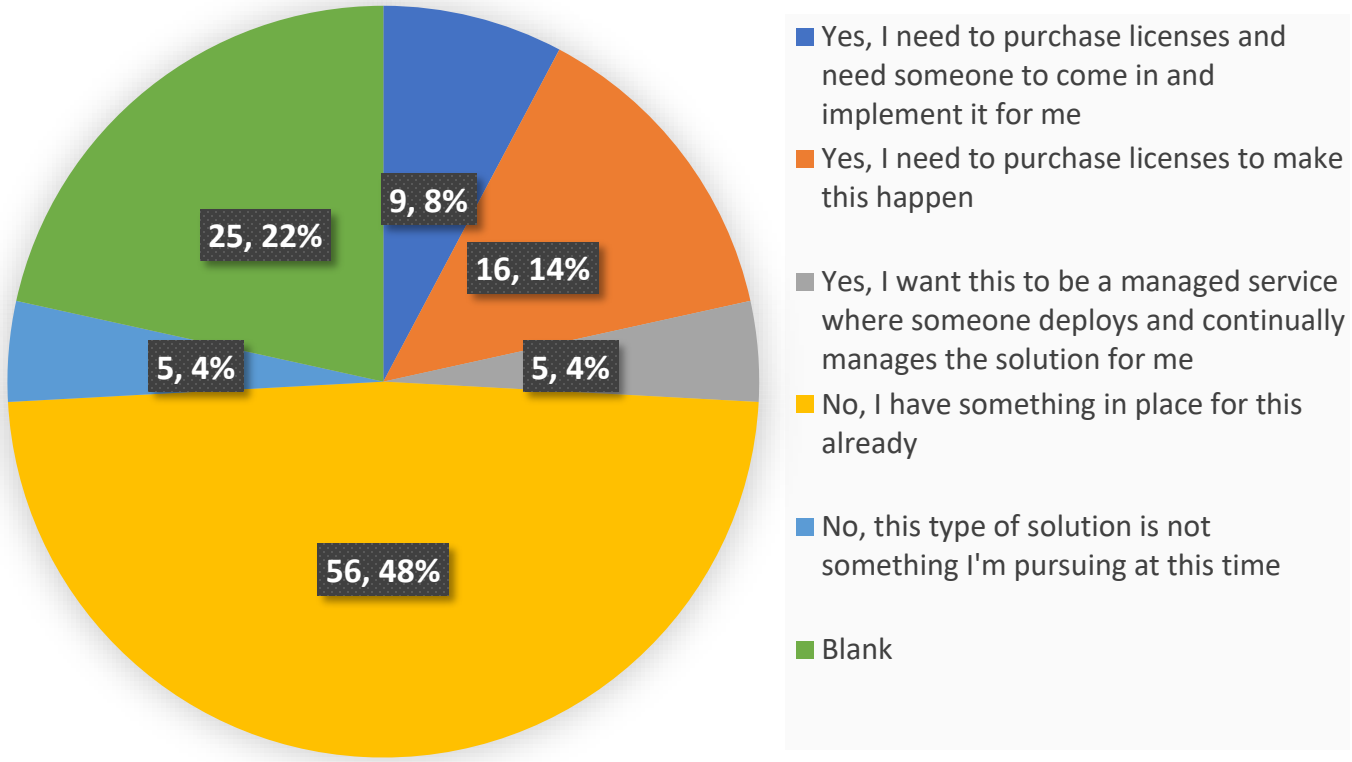
Objective 1.5 - Identify all government websites and migrate non .gov sites to .gov domains

For this objective, do you need third-party assistance to migrate or implement a .gov presence?

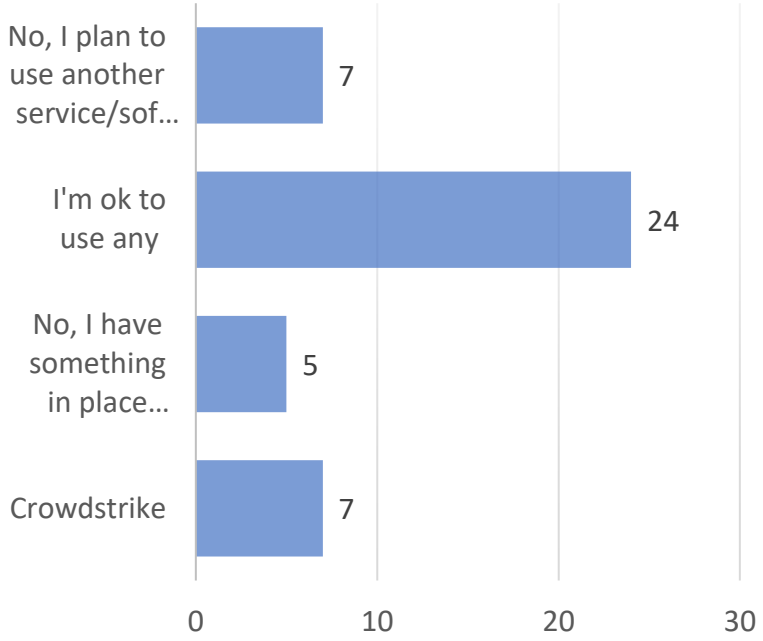


Objective 2.1 - Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers

For this objective, are you looking for an endpoint detection and response solution?

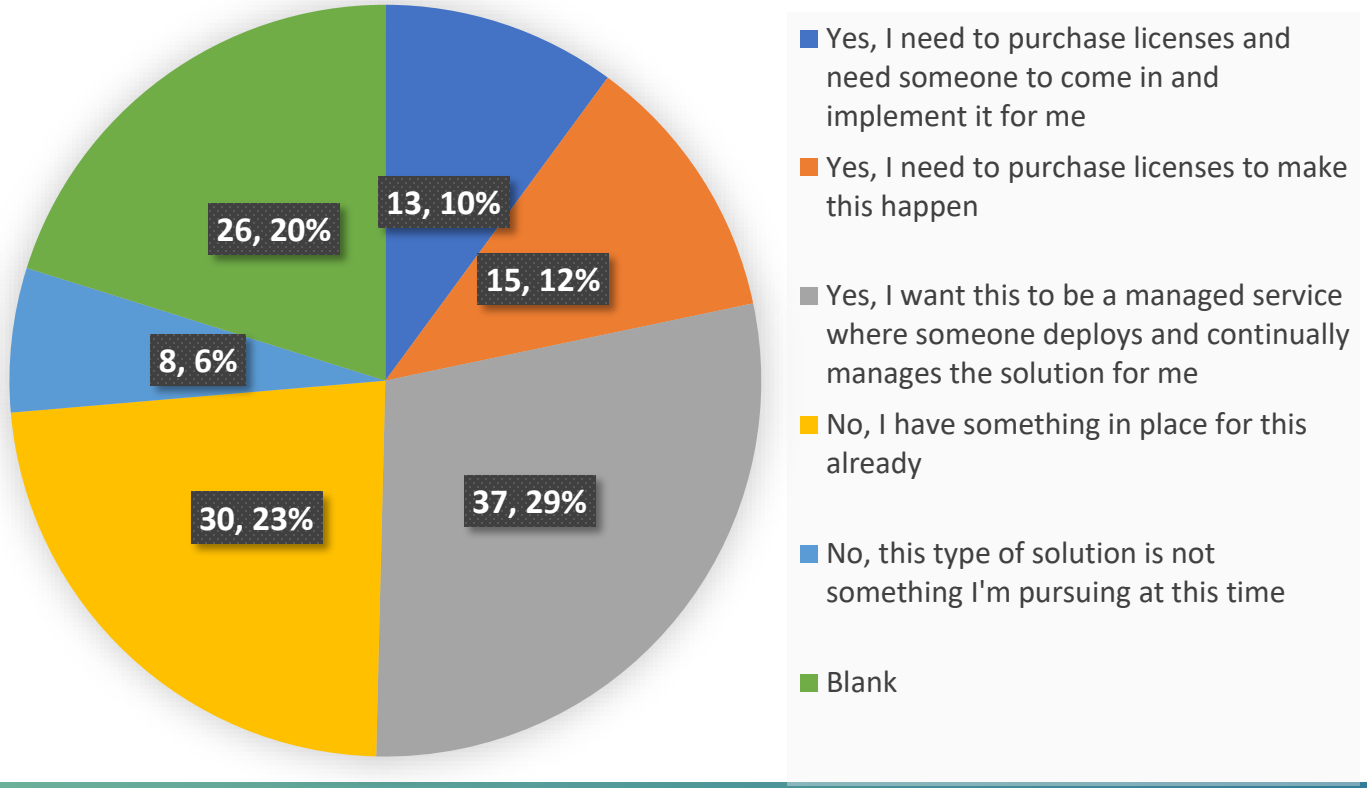


Would you plan to use any of the following software and/or services for this solution?

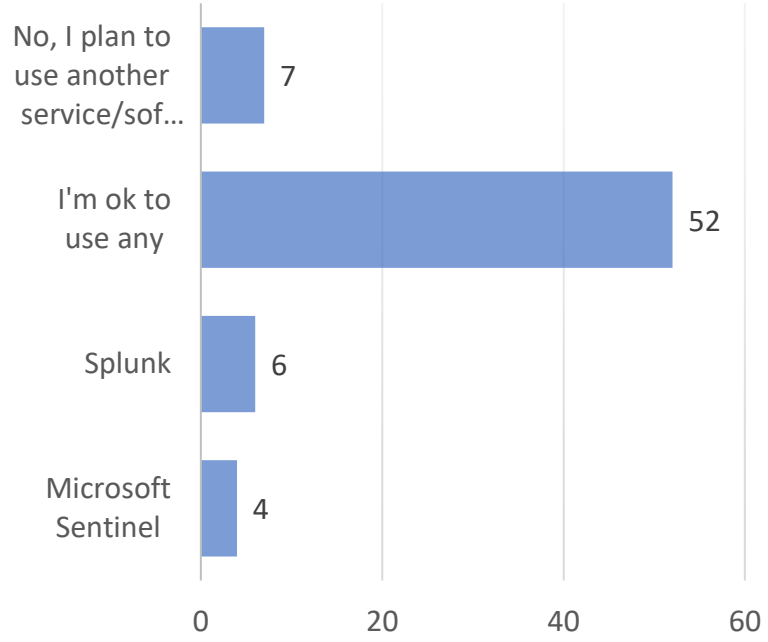


Objective 2.3 - Centralize security event alerting

For this objective, are you looking for a security information and event management (SIEM) solution for your environment?

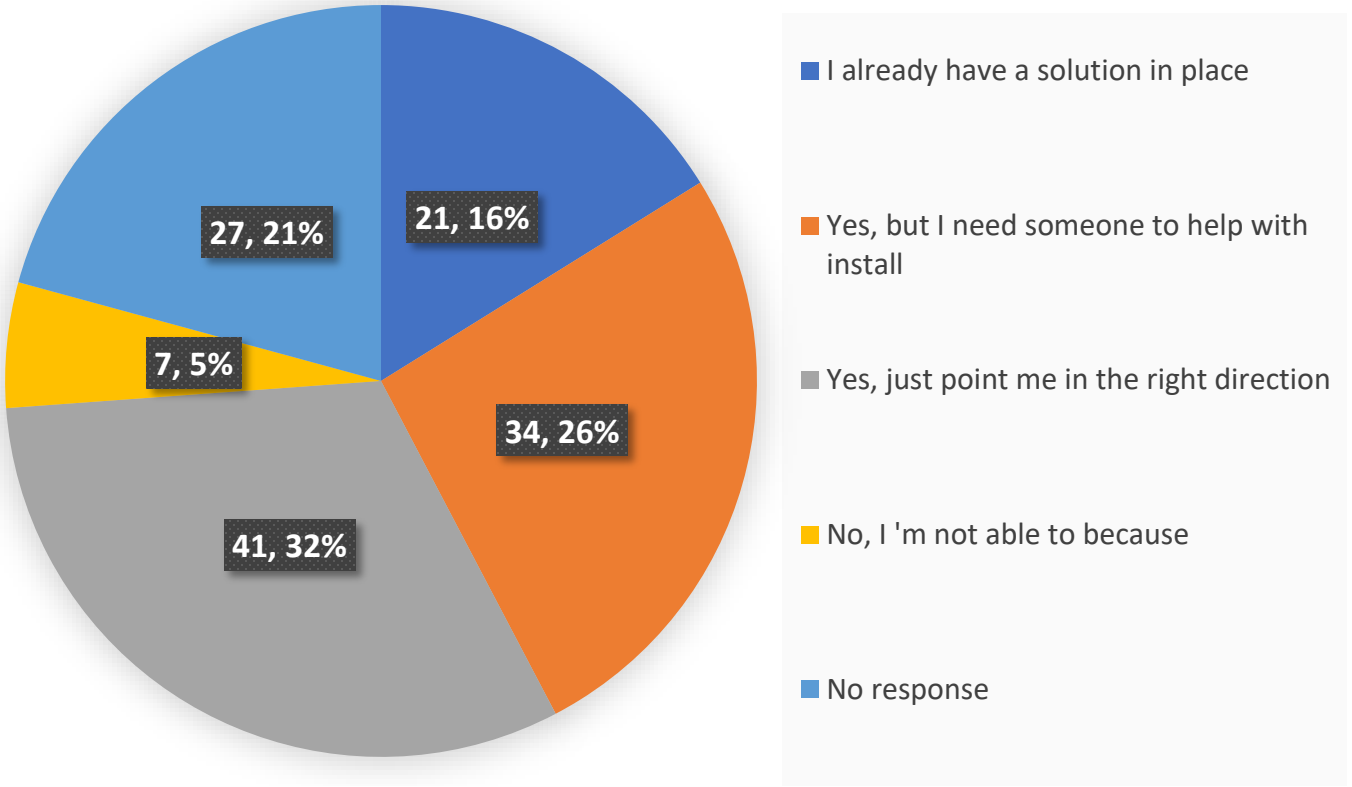


Would you plan to use any of the following software and/or services for this solution?



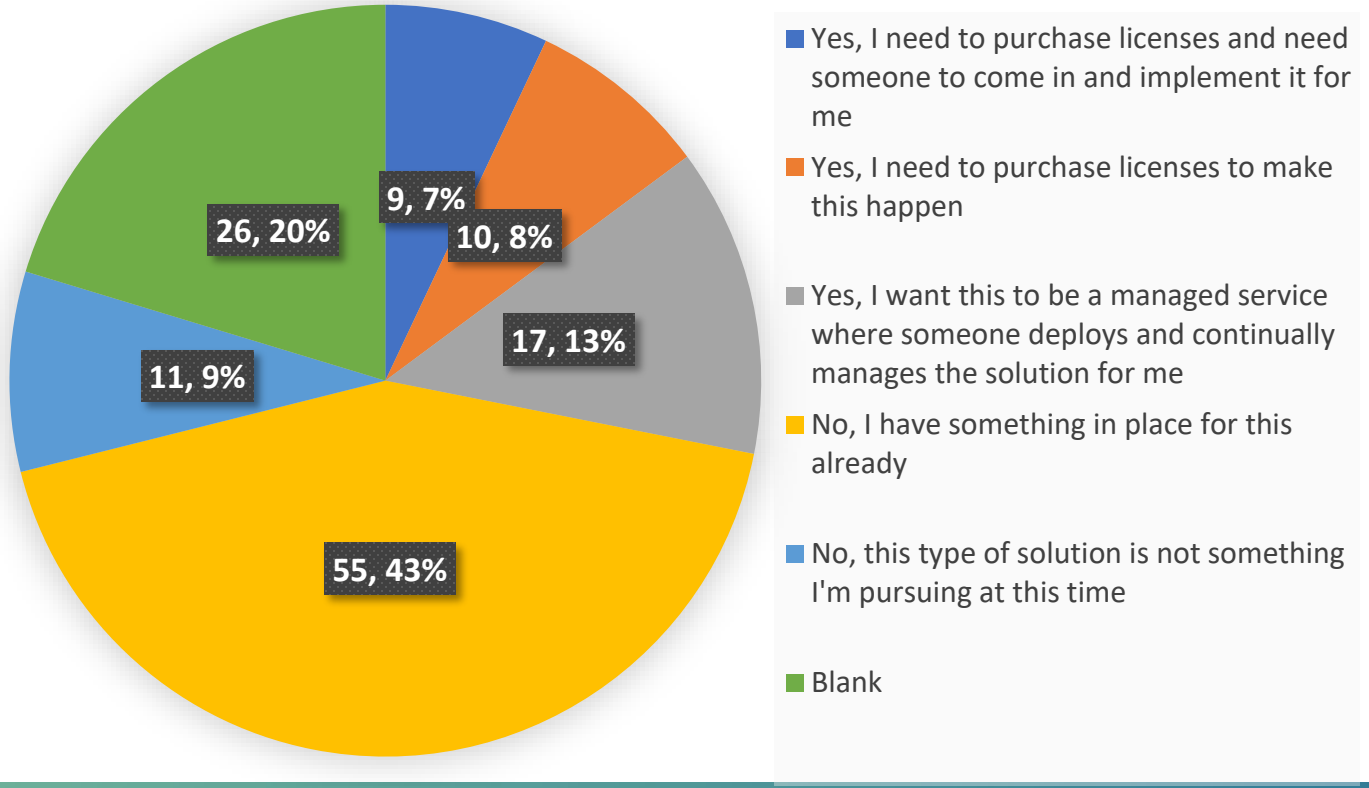
Objective 2.4 - Collect network traffic flow logs

For this objective, are you able to deploy or have a third-party deploy the MS-ISAC monitoring solution Albert?

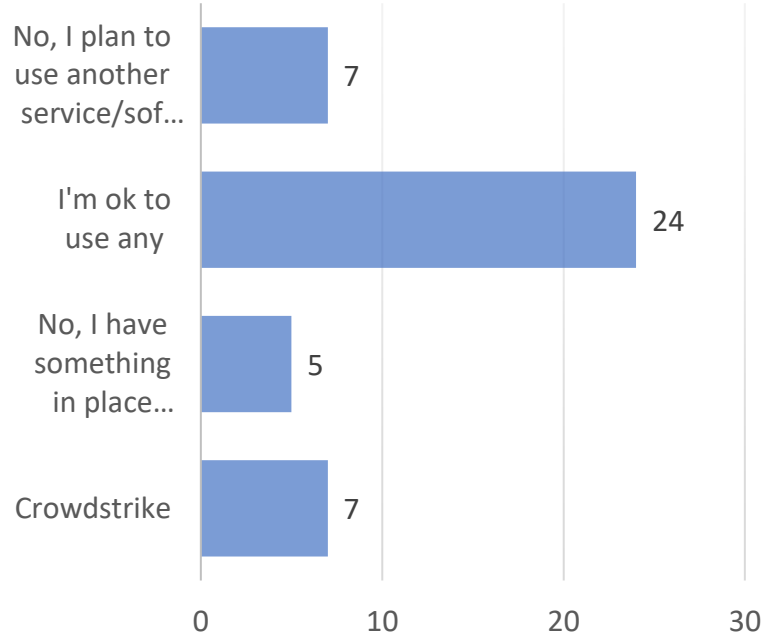


Objective 3.1 - Implement and manage firewalls on all end point devices (i.e. user workstations, servers)

For this objective, are you looking for an endpoint (workstation and/or server) managed firewall solution?



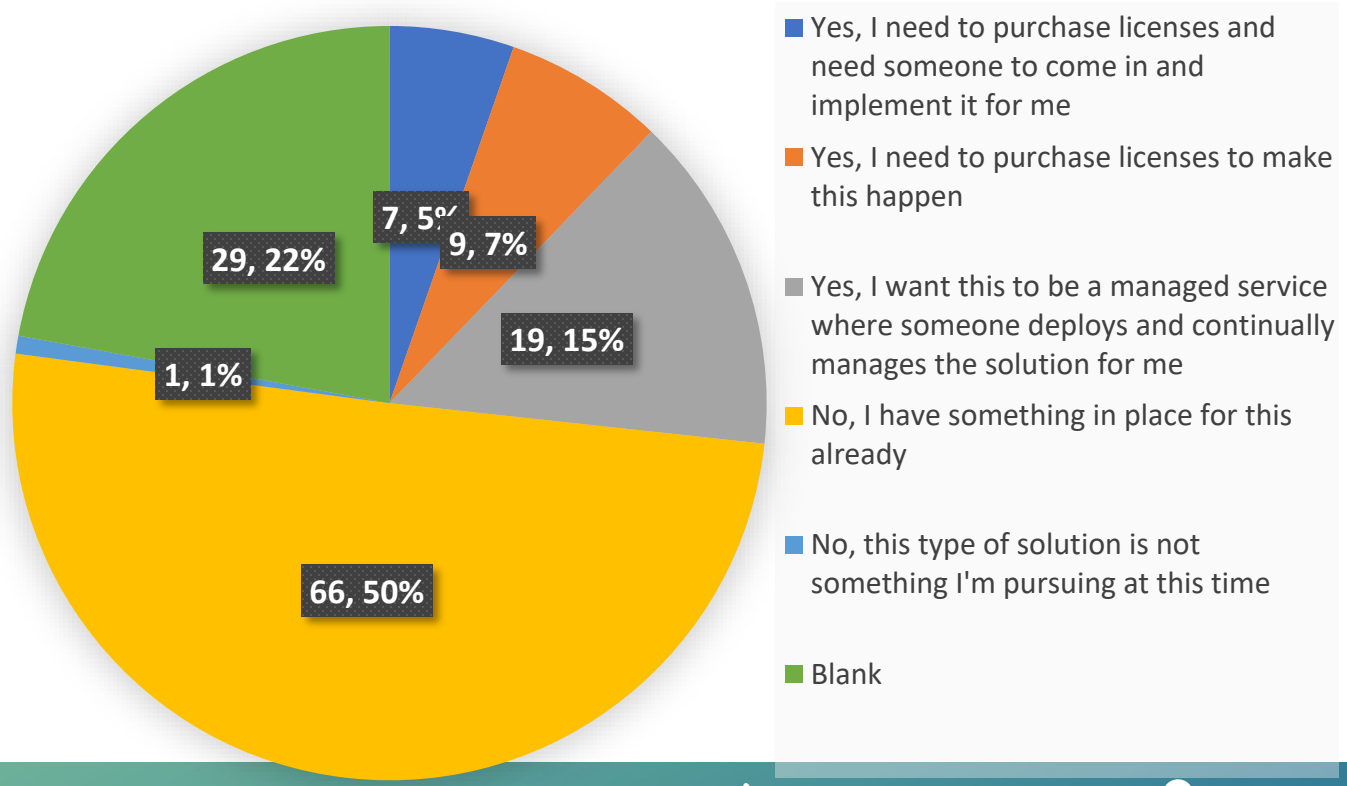
Would you plan to use any of the following software and/or services for this solution?



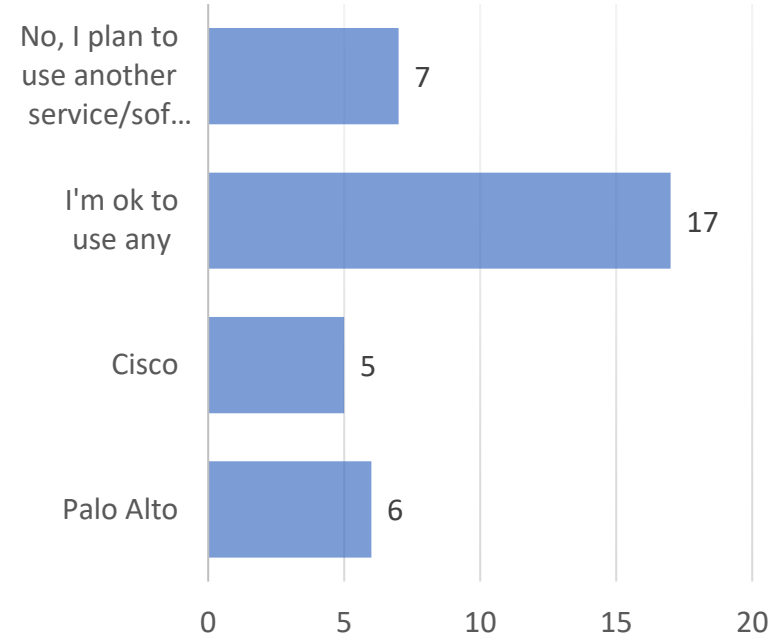
Objective 3.2 - Implement and manage network firewalls for ingress and egress points

Objective 2.2 - Deploy network monitoring, filtering and detection at network egress and ingress points

For this objective, are you looking for a network monitoring and firewall solution for your network?

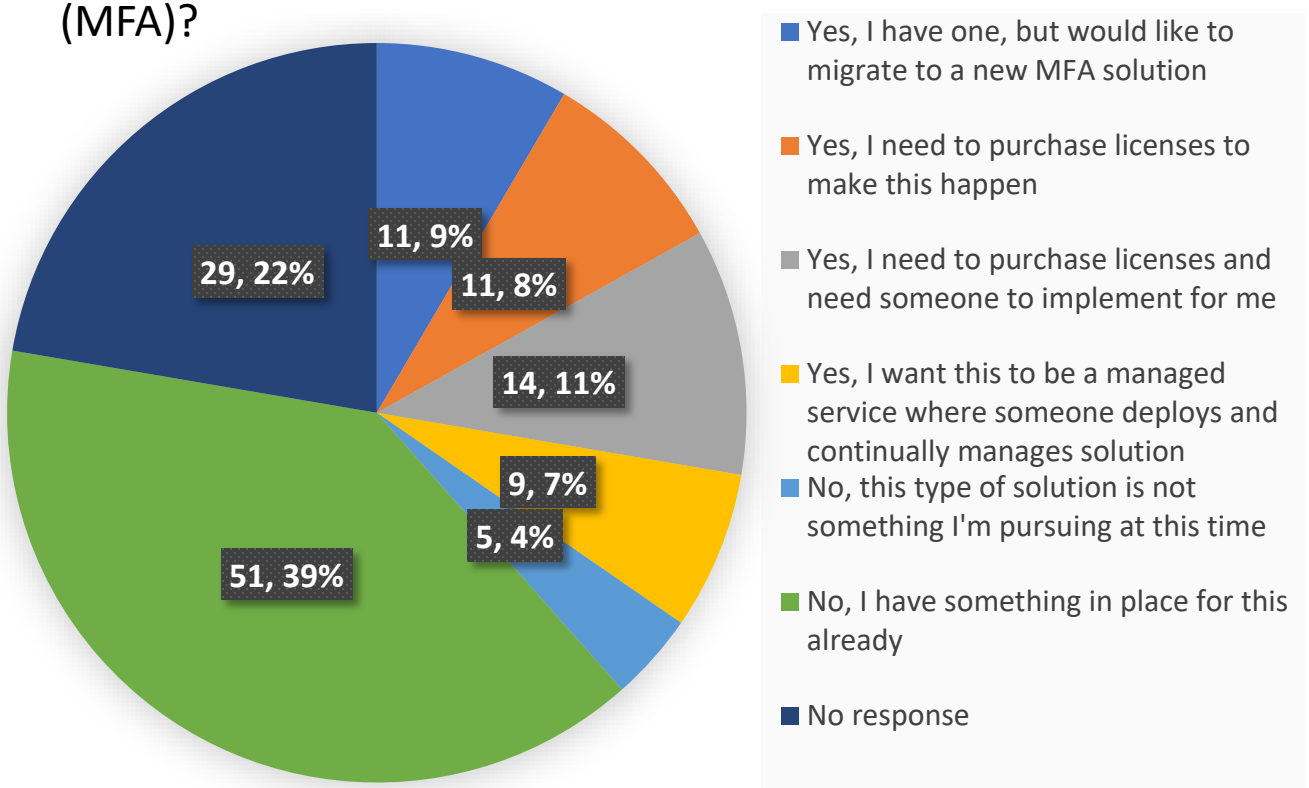


Would you plan to use any of the following software and/or services for this solution?

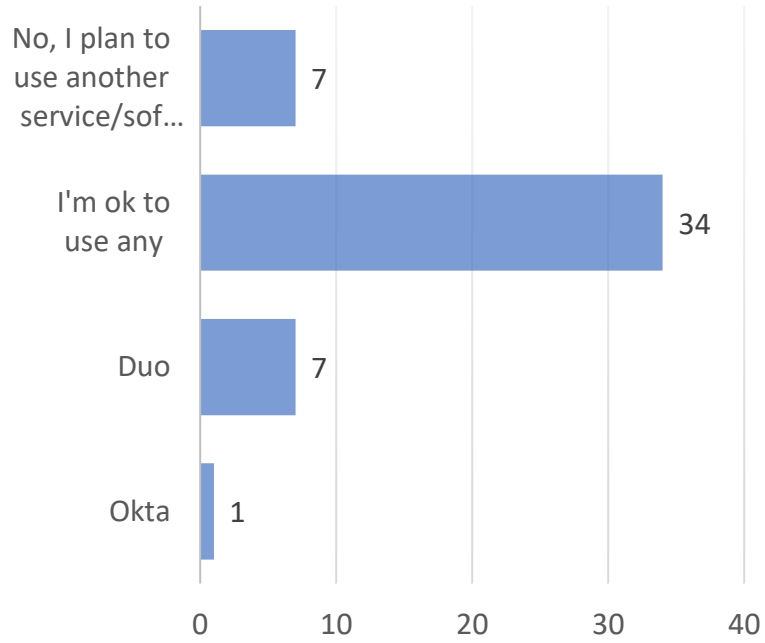


Objective 3.4 - Multifactor authentication (MFA) implementation for compatible externally exposed systems, network access and/or administrative access

For this objective, are you looking for a multifactor authentication solution (MFA)?

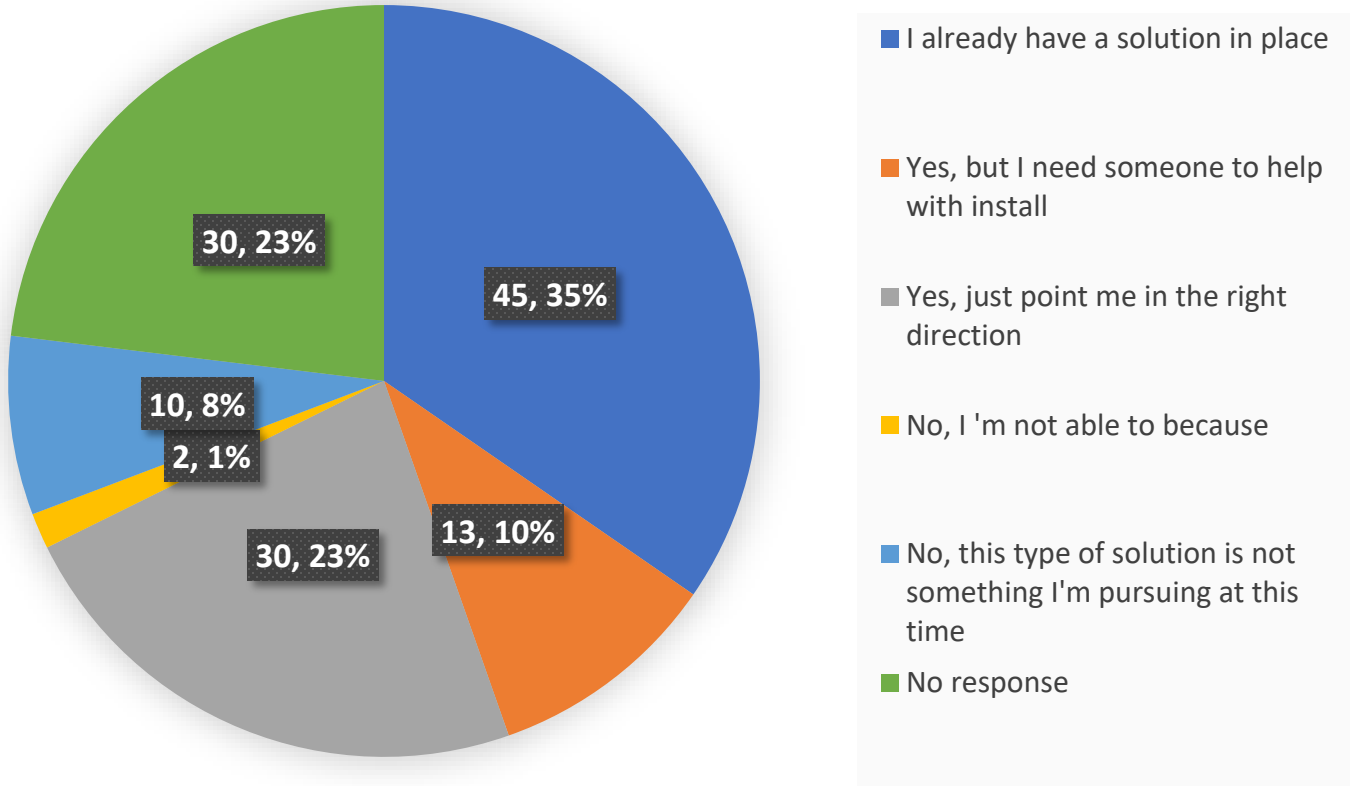


Would you plan to use any of the following software and/or services for this solution?



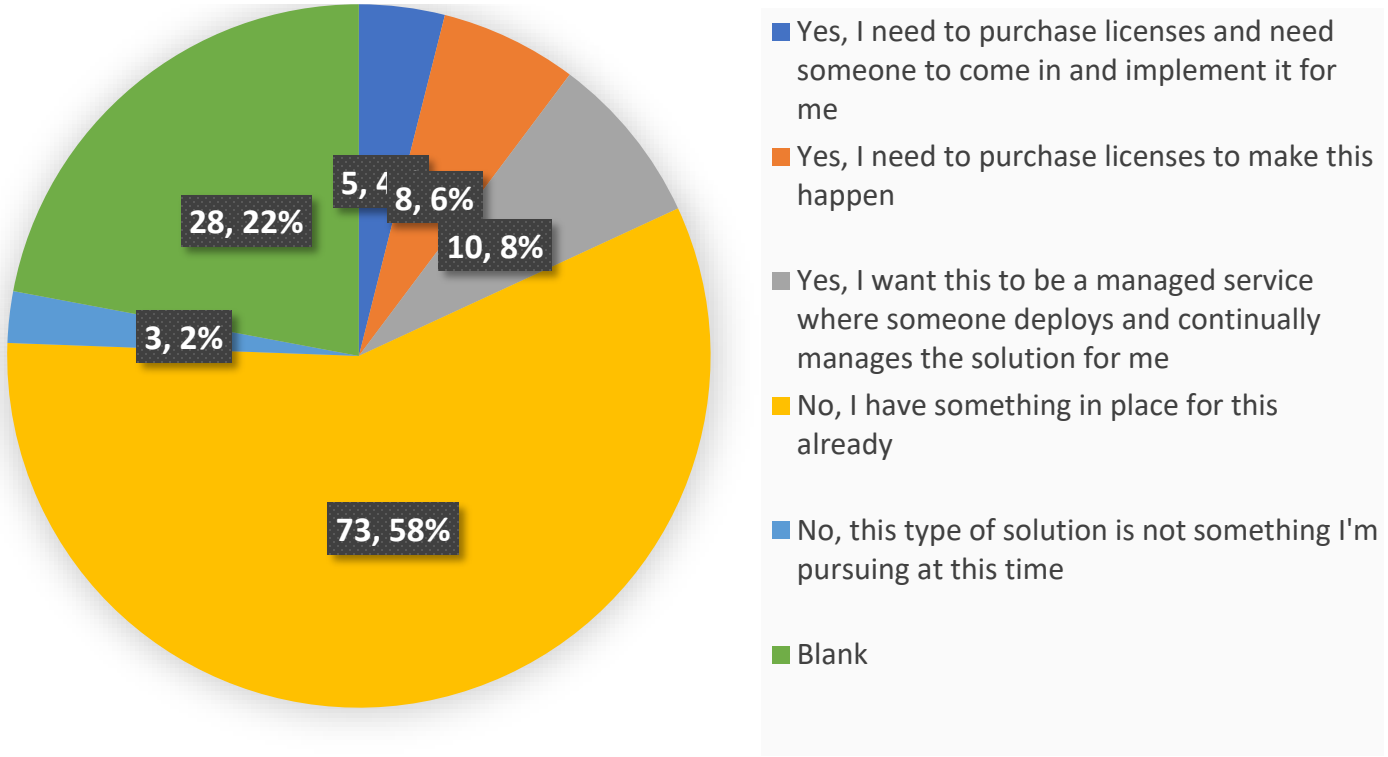
Objective 3.5 - Domain name system (DNS) filtering/firewall

Are you able to enroll in the malicious domain blocking and reporting tool provided by MS-ISAC?

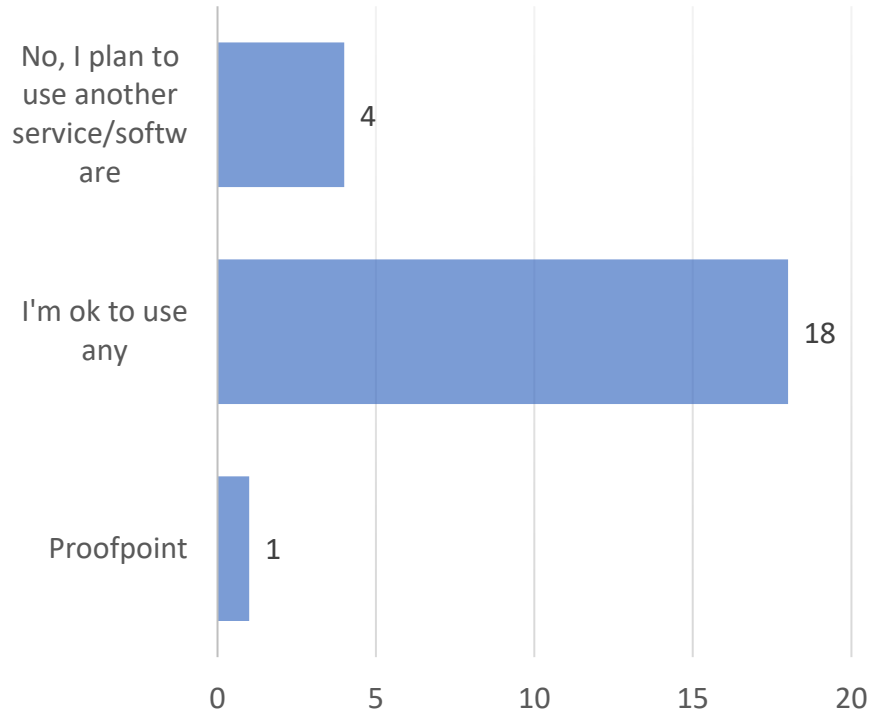


Objective 3.6 - Email filtering and protection

For this objective, are you looking for an email filtering solution?

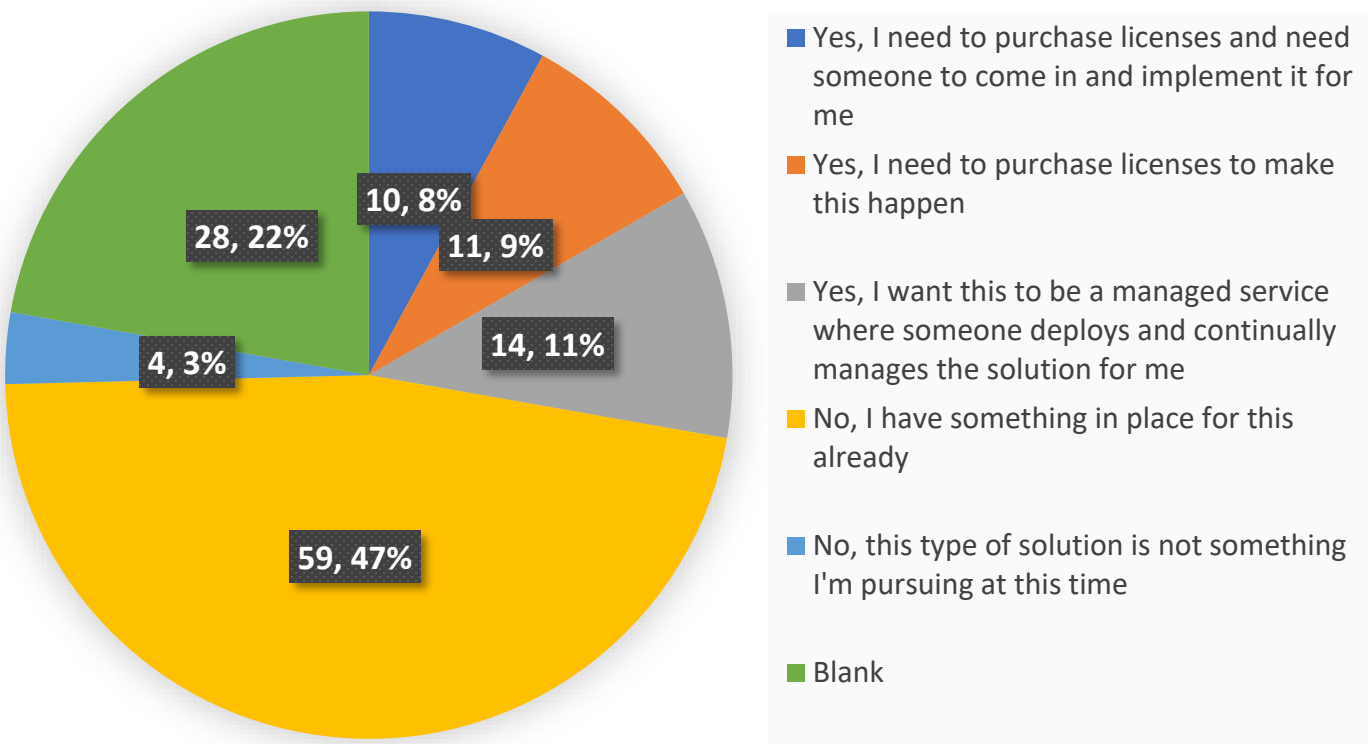


Would you plan to use any of the following software and/or services for this solution?

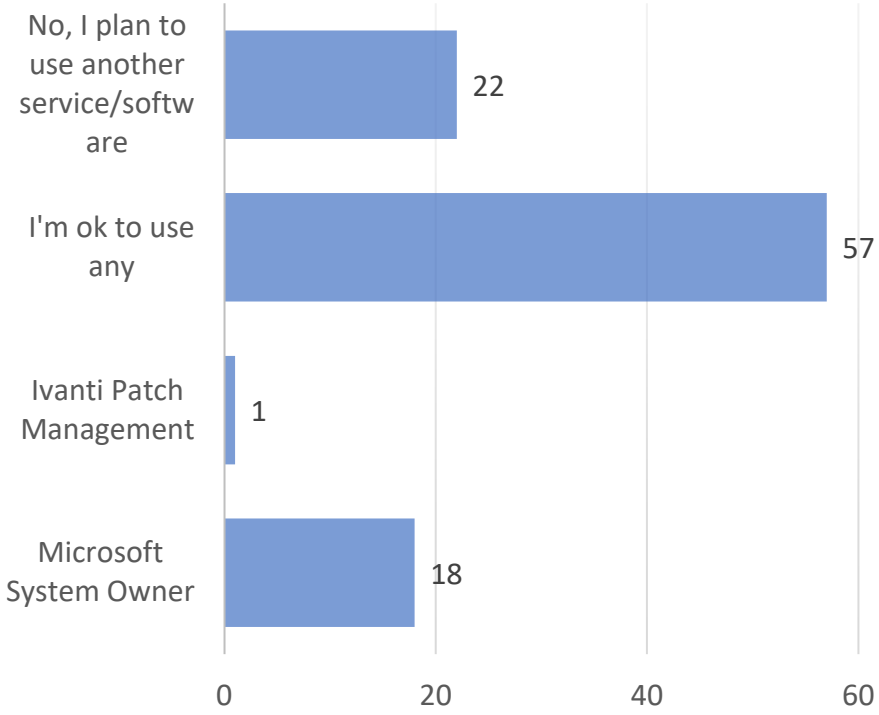


Objective 3.9 - Ensure patch management program is implemented and up to date

For this objective, are you looking for a solution to help deploy patches to your environment?

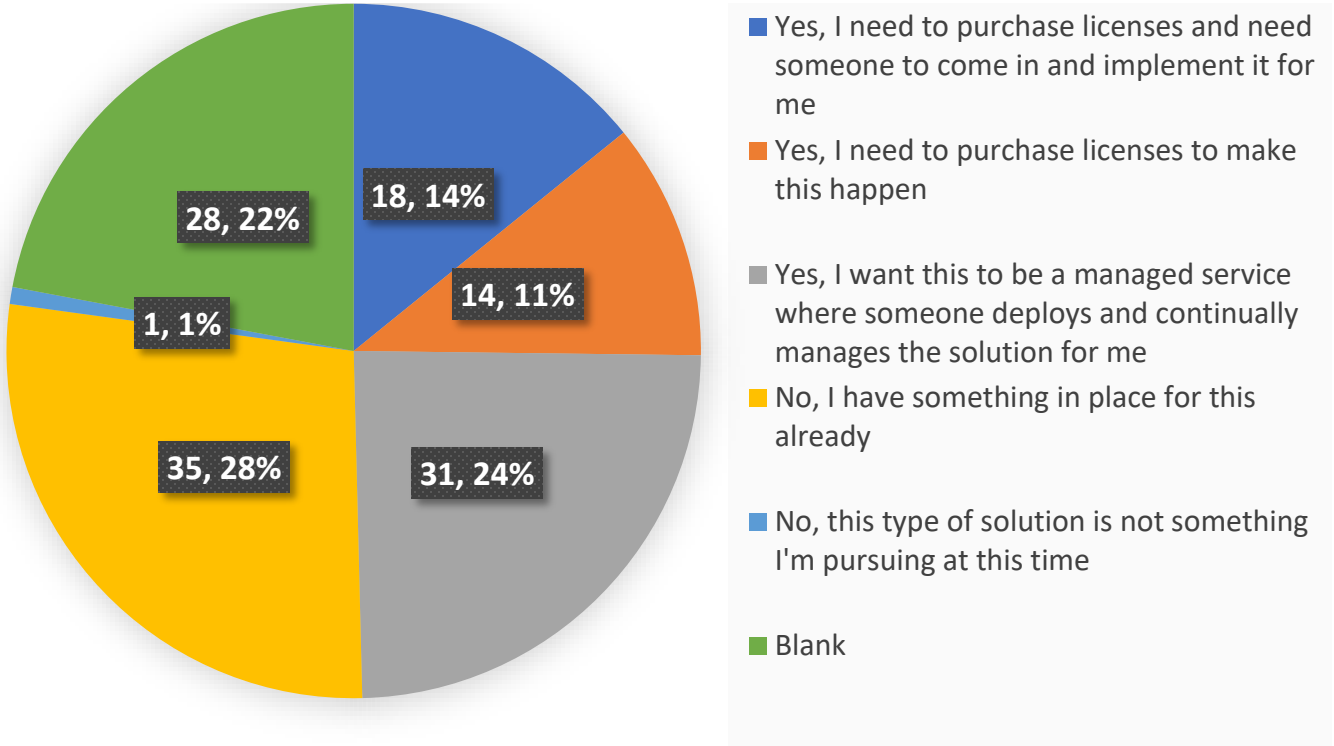


Would you plan to use any of the following software and/or services for this solution?

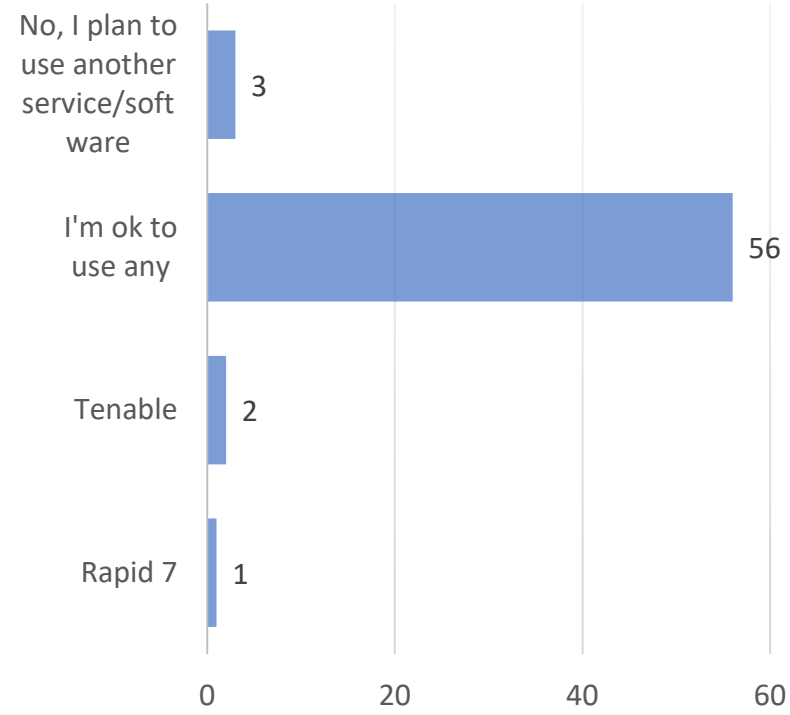


Objective 5.2 - Perform automated vulnerability scans

For this objective, are you looking for vulnerability scanning solution?



Would you plan to use any of the following software and/or services for this solution?



STATE AND LOCAL CYBERSECURITY GRANT PROGRAM PROCUREMENT GUIDELINES USING STATEWIDE TECHNOLOGY CONTRACTS

VITA has developed value-driven statewide IT contracts that enable users to benefit their organization and Virginians by consolidating and leveraging the Commonwealth's buying power. These contracts may be utilized by public bodies for the purposes of the State and Local Cybersecurity Grant Program (SLCGP).

More information and resources regarding VITA's statewide contracts are available on the VITA website under the procurement tab.

Specific suppliers that are identified in the Cyber Planning Objectives below include authorized resellers that are under state contract. For example, Thundercat and SHI have statewide contracts that are available for public bodies use. While these contracts are available for your use, there may be additional cooperative contracts that fit your business need such as GSA Technology Cooperative contracts.

Executive Branch Agencies have specific instructions for use detailed on the VITA website under each contract.

While other public bodies can adopt those instructions, they must adhere to their respective procurement policies.

General instructions for use of these contracts include but are not limited to:

- Identify the contract for use from the list of contracts on the VITA's website.
- Identify the suppliers' account representative who is listed for the respective contract.
- Send a Request for quote (RFQ) for any combination of solution, product, or services provided under the established contracts to the supplier's account representative.
- If a public body determines that a Competitive Request for Quote (CRFQ) is required to ensure it receives the best value for any combination of its needed product, solution, or services under the contract, then the public body may, at is sole discretion, use the CRFQ process to obtain identical or similar solutions, products, or services to those provided by a supplier pursuant to the identified contract. The CRFQ will clearly outline the project timing and requirements. If the public body is not able to identify the exact specifications required, then the CRFQ respondents will be given the opportunity to identify and propose their recommended specifications.
- Public entities may use the Statement of Work templates listed under each contract for their own use.

- Virginia Public bodies desiring to use the SLCGP must ensure that any statement of work (SOW) or contract procured contains the applicable federal terms and conditions required by the grant. And follow their respective procurement policies should there be a conflict with the federal terms and conditions and the Virgina Public Procurement Act (VPPA). The Federal terms and conditions are listed at the end of this document.

These guidelines do not imply that VITA contracts fulfill the SLCGP requirements. It is the sole responsibility of the public body using the VITA statewide contracts to ensure the procurement aligns with the SLCGP requirements.

INITIAL CYBER PLANNING OBJECTIVES

OBJECTIVE: 1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software)

Configuration Management Database (CMDB): stores information about all technology assets, including hardware, software, and their configurations

- ServiceNow CMDB-**ECOS/THUNDERCAT**
- Atlassian – **GSA through Carahsoft**

IT Asset Management (ITAM) Software: track and manage technology assets throughout their lifecycle, including procurement, deployment, maintenance, and retirement

- Atlassian Jira Service Management – **GSA through Carahsoft**
- ServiceNow ITAM - **SHI**
- RunZero- **GSA through Carahsoft**

Network Monitoring Tools: automatically discover and inventory network-connected devices, such as routers, switches, servers, and network-attached devices

- SolarWinds Network Performance Monitor- **THUNDERCAT**
- Nagios- **THUNDERCAT**

Software Asset Management (SAM) Tools: monitor and manage software installations, providing visibility into software assets across the enterprise

- RunZero – **GSA through Carahsoft**
- Snow Software-**SHI**

IT Service Management (ITSM) Tools: to track technology assets and their associated service requests, incidents, and changes

- ServiceNow ITSM - **SHI**
- Atlassian Jira Service Management- **GSA through Carahsoft**

Vulnerability Management Tools: perform regular scans and assessments of technology assets, identifying vulnerabilities and providing insights into the security posture of the assets

- Tenable.io- **THUNDERCAT**
- Rapid7 InsightVM-**SHI**

Automated Discovery Tools: automatically scan and discover technology assets on the network, providing detailed information about hardware, software, configurations, and dependencies

- ServiceNow - **SHI**
- RunZero – **GSA through Carahsoft**
- Axonius- **SHI**
- Atlassian – **GSA through Carahsoft**

OBJECTIVE: 1.2 Upgrade or replace all software no longer receiving security maintenance/support

Patch Management Systems: automate the process of applying software patches and updates, ensuring that unsupported software is replaced or upgraded with supported versions

- SolarWinds Patch Manager- **SHI & THUNDERCAT** HAS SOLARWIND PUBLISHER
- Microsoft Systems Center – **SHI has the publisher**
- Ivanti Patch Management- **SHI has the publisher**

Software Deployment and Distribution Systems: facilitate the deployment of new software versions or replacements to end-user devices, ensuring that unsupported software is replaced with supported alternatives.

- Microsoft System Center Configuration Manager (SCCM)- **SHI has the publisher**
- Ivanti Endpoint Manager- **SHI has the publisher**

Configuration Management Systems: assist in managing and controlling software versions, allowing organizations to enforce policies that prevent the use of unsupported software and promote the adoption of supported alternatives

- Puppet- **SHI has the publisher**
- Ansible – Red Hat **GSA through Carahsoft/SHI**
- Microsoft System Center – **SHI has the publisher**

Software Asset Management (SAM) Tools: organizations identify software that is no longer supported and provide insights into suitable replacement options

- Snow Software -**SHI has the publisher**
- Flexera Software Asset Management- **SHI and ECOS has the publisher**
- ServiceNow SAM Pro- **ECOS, SHI, & THUNDERCAT has Servicenow publisher**

Enterprise Architecture Tools: enable organizations to assess and plan their technology landscape, identifying unsupported software and recommending alternative solutions

- IBM Rational System Architect- **THUNDERCAT has the publisher**
- Ardoq - **ECOS**

Vendor and Supplier Management Systems: assist in managing relationships with software vendors and suppliers, ensuring that organizations are aware of software end-of-life dates and can plan for upgrades or replacements accordingly

- Flexera – **GSA through Carahsoft**

OBJECTIVE: 1.3 Identify all government websites and migrate non .gov sites to .gov domains

- Domain Name System (DNS) monitoring and management tools:
- Cloudflare - **GSA through GovPlace**
- Infoblox- **THUNDERCAT**
- Cisco Umbrella - **GSA**
- Sitecore-**SHI**

OBJECTIVE: 2.1 Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers

- CrowdStrike Falcon- **ECOSS/SHI**

OBJECTIVE: 2.2 Deploy network monitoring, filtering and detection at network egress and ingress points

- Cisco Firepower NGFW (Next-Generation Firewall)- **SHI**
- Palo Alto Networks Next-Generation Firewall- **THUNDERCAT/ SHI**
- Fortinet FortiGate - **SHI publisher**
- McAfee/Trellix Network Security Platform- **THUNDERCAT/SHI**

OBJECTIVE: 2.3 Centralize security event alerting

- Splunk Enterprise Security- **THUNDERCAT/SHI/ECOSS**
- Microsoft Sentinel – **GSA through Carahsoft**
- Google Chronicle – **GSA through Carahsoft**

OBJECTIVE: 2.4 Collect network traffic flow logs

- Albert Sensor – **MS-ISAC/DHS**

Objective: 3.1 Implement and manage firewalls on all end point devices (i.e. user workstations, servers)

- CrowdStrike Falcon- **ECOSS/SHI**

Objective: 3.2 Implement and manage network firewalls for ingress and egress points

- Cisco ASA (Adaptive Security Appliance)- **THUNDERCAT and SHI has the publisher**
- Palo Alto Networks Next-Generation Firewall- **THUNDERCAT and SHI has the publisher**
- Fortinet FortiGate-**SHI**

Objective: 3.3 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access

- Duo Security-**SHI**
- Cyberark – **GSA**
- Okta Verify- **THUNDERCAT**
- YubiKey- **GSA**
- Ping Identity – **GSA**

Objective: 3.4 Domain Name System (DNS) Filtering/Firewall

- Cisco Umbrella (formerly OpenDNS) – MDBR via MS-ISAC - **GSA**

Objective: 3.5 Email filtering and protection

- Proofpoint- **THUNDERCAT**/**SHI**
- Area 1 **– Cloudflare - GSA**

Objective: 3.6 Ensure patch management program is implemented and up to date

- Microsoft System Center Configuration Manager (SCCM)- **SHI has the publisher**
- SolarWinds Patch Manager- **THUNDERCAT has the publisher**
- Ivanti Patch for Windows- **SHI has the publisher**

Objective 4.1: Identify security gaps associated with program objectives which can be supported by the grant program

- Provided through VITA Services - CAI

Objective 5.1: Network and system architecture diagram and assessment

- Lucidchart- **ECOS**
- Microsoft Visio- **SHI** Publisher
- SolarWinds Network Topology Mapper- **THUNDERCAT**

OTHER OBJECTIVES

OBJECTIVE: 1.1 Ensure only authorized assets connect to enterprise systems and are inventoried

Network Access Control (NAC) Systems: enforce security policies to control and authenticate devices attempting to connect to the network, allowing only authorized assets to gain access

- Cisco Identity Services Engine (ISE)- **THUNDERCAT**
- ForeScout CounterACT- **THUNDERCAT**

Endpoint Protection Platforms (EPP): restrict unauthorized assets from connecting to enterprise systems

- CrowdStrike Falcon-**ECOSS/SHI**

Identity and Access Management (IAM) Systems: manage user identities and access rights, helping to ensure that only authorized individuals can access enterprise systems and their associated assets

- Okta- **THUNDERCAT/SHI**
- Duo – **SHI**

Intrusion Detection and Prevention Systems (IDPS): detect and block unauthorized devices attempting to connect to the network or access enterprise systems

- Snort - **GSA**
- Suricata **– GSA**
- Palo Alto – **GSA through Carahsoft**

Security Information and Event Management (SIEM) Systems: centralized monitoring and analysis of security events, enabling the detection of unauthorized access attempts or anomalous behavior from assets

- Splunk Enterprise Security- **THUNDERCAT/SHI/ECOSS**
- Microsoft Sentinel – **GSA through Carahsoft**
- Google Chronicle **– GSA through Carahsoft**

OBJECTIVE: 1.2 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business

DLP Systems: identify and monitor sensitive data within an organization's systems. They can scan and classify data based on predefined rules and policies, enabling organizations to maintain an inventory of their sensitive data

- Symantec Data Loss Prevention- **THUNDERCAT has the publisher**
- McAfee Data Loss Prevention- **THUNDERCAT and SHI has the publisher**
- Forcepoint DLP – **GSA through Carahsoft**
- Digital Guardian Data Loss Prevention**- SHI has the publisher**

Data Discovery Tools: scan an organization's network, storage devices, and databases to identify and catalog sensitive data. They can help establish a comprehensive data inventory by locating data at rest, in transit, or even within cloud services

- Varonis Data Classification Framework- **SHI has the publisher**
- Spirion Sensitive Data Manager
- IBM Security Guardium- **THUNDERCAT has the publisher**
- Stealthbits Data Discovery and Classification- **SHI has the publisher**

SIEM Systems: collect and analyze security event logs from various systems and applications across an organization's network. By correlating and analyzing these logs, SIEM systems can provide insights into potential data breaches or unauthorized access, facilitating data inventory management.

- Splunk Enterprise Security- **THUNDERCAT/SHI/ECOSS**
- Google Chronicle – **GSA through Carahsoft**
- Microsoft Sentinel – **GSA through Carahsoft**

Vulnerability Management Systems: systems scan and assess an organization's systems, applications, and networks for known vulnerabilities. By identifying potential weaknesses, organizations can proactively address them and prevent unauthorized access to sensitive data.

- Qualys Vulnerability Management- **THUNDERCAT and SHI has the publisher**
- Tenable.io- **THUNDERCAT**
- Rapid7 InsightVM- **THUNDERCAT and ECOS has the publisher**

Access Control Systems: help ensure that only authorized individuals can access sensitive data. Implementing these systems helps maintain data inventory and restrict access to sensitive information.

- Okta - **THUNDERCAT/SHI PUBLISHER**
- CyberArk - **GSA**
- Ping Identity - **GSA**

Encryption and Data Protection: Encrypting sensitive data both at rest and in transit provides an additional layer of protection.

- Symantec Endpoint Encryption- **THUNDERCAT/SHI**
- BitLocker (Microsoft Windows) - **GSA**
- Sophos SafeGuard Encryption- **THUNDERCAT/SHI PUBLISHER**

Data Loss Incident Response: incident response plan for data loss incidents helps organizations detect, respond to, and recover from data breaches.

- IBM Resilient Incident Response Platform- **THUNDERCAT has the publisher splunk**
- Splunk Phantom- **THUNDERCAT/SHI/ECOSS**
- RSA NetWitness Orchestrator- **THUNDERCAT/SHI has the publisher**
- CyberSponse Security Orchestration, Automation, and Response (SOAR) **– GSA through Carahsoft**

OBJECTIVE: 1.3 Establish and maintain inventory of administrator, service and user accounts

Identity and Access Management (IAM) Systems: manage user identities and access rights, helping to ensure that only authorized individuals can access enterprise systems and their associated assets.

- Okta**- THUNDERCAT/SHI**
- Splunk Enterprise Security- **THUNDERCAT/SHI/ECOSS**
- Crowdstrike Identity – **GSA through Carahsoft**
- ServiceNow CMDB-**ECOS/THUNDERCAT**
- SolarWinds Service Desk- **THUNDERCAT**

OBJECTIVE: 2.1 Audit log collection for all servers and systems hosting data in accordance with log management standards

- Splunk Enterprise Security- **GSA**
- Microsoft Sentinel - **SHI**
- Google Chronicle - **THUNDERCAT**

OBJECTIVE: 2.2 Web application firewall

- Imperva WAF-**ECOS/SHI/THUNDERCAT**
- Cloudflare WAF - **GSA**
- Akamai Web Application Protector- **THUNDERCAT**
- AWS WAF (Amazon Web Services Web Application Firewall) – **GSA MAS**

Objective: 3.1 Encrypt sensitive data in transit and on devices hosting sensitive data

- Palo Alto GlobalProtect **– SHI**
- Zscaler – **SHI/GSA**

Objective: 3.2 Centralized authentication and authorization (Single Sign On)

- Okta- **THUNDERCAT** and **SHI**
- Ping Identity**-ECOS has the vendor**

Objective: 3.3 Content and malicious traffic filtering through anti-virus and threat detection software

- CrowdStrike Falcon- **ECOS**S/**SHI**
- VirSec - **Thundercat**

Objective 4.1: Establish and maintain a data recovery process

- Veeam Backup & Replication- **SHI**/ **THUNDERCAT**
- Commvault Complete Backup & Recovery- **SHI/ THUNDERCAT has the publisher**
- Veritas NetBackup- **SHI**/ **THUNDERCAT**
- Acronis Cyber Backup- **SHI has the publisher**
- Dell EMC Data Protection Suite- **SHI has the publisher**
- Rubrik Cloud Data Management - **GSA**
- Arcserve Unified Data Protection- **SHI has the publisher**
- IBM Spectrum Protect- **THUNDERCAT has the publisher**
- Cohesity DataProtect- **SHI has the publisher**
- Unitrends Backup- **SHI**

Objective 4.2: Establish and maintain an isolated/vaulted instance of recovery data

- Azure Blob Storage- **ECOS**
- AWS Glacier **- GSA**
- Google Cloud Storage Coldline - **SHI**
- IBM Cloud Object Storage- **THUNDERCAT has the publisher**
- Oracle Archive Storage - **GSA**
- Backblaze B2 Cloud Storage - **GSA**
- Wasabi Hot Cloud Storage- **SHI has the publisher**
- Synology C2 Backup - **GSA**
- Dropbox Business Advanced- **SHI has the publisher**
- Box Enterprise – **SHI**

Objective 4.3: Implement disaster recovery and data recovery testing

- CloudEndure Disaster Recovery **/AWS GSA**
- VMware Site Recovery Manager - **GSA**
- Zerto Virtual Replication- **SHI has the publisher**
- Carbonite Recover- **SHI has the publisher**
- Unitrends Disaster Recovery as a Service (DRaaS)- **SHI**
- Druva Phoenix - **GSA**
- Quorum onQ
- Infrascale Disaster Recovery
- Microsoft Azure Site Recovery-**ECOS has publisher**
- RapidScale Disaster Recovery as a Service

Objective 4.4: Implement technology to support continuity of services in the case of a natural disaster or cyber-attack.

- F5 BIG-IP Load Balancer- **THUNDERCAT/SHI**
- Citrix ADC (formerly NetScaler)- **THUNDERCAT/SHI**
- Barracuda CloudGen Firewall- **THUNDERCAT/SHI**
- Palo Alto Networks VM-Series Firewall- **THUNDERCAT/SHI**
- Cisco Umbrella (formerly OpenDNS) - **GSA**
- Fortinet FortiGate Next-Generation Firewall- **SHI has publisher**
- Sophos XG Firewall- **THUNDERCAT** and **SHI has the publisher**
- Check Point CloudGuard- **SHI has publisher**
- Juniper Networks SRX Series Services Gateways- **SHI has publisher**
- SonicWall Network Security Appliance- **THUNDERCAT and SHI has the publisher**

Objective 5.1: Perform automated vulnerability scans

- Burp Suite Professional **– Portswigger SHI**
- Metasploit Framework – Rapid 7 - **SHI**
- Acunetix Vulnerability Scanner- **SHI has Publisher**
- Retina Network Community – Beyond Trust - **SHI**
- Qualys Vulnerability Management- **THUNDERCAT/SHI**
- Rapid7 Nexpose Vulnerability Scanner- **THUNDERCAT and ECOS has the publisher**
- Tenable.io Vulnerability Management- **THUNDERCAT**
- Nessus Essentials- **SHI has the publisher**
- Nessus Vulnerability Scanner **– SHI**
- Acunetix Vulnerability Scanner- **SHI has Publisher**

FY 23 DHS Standard Terms and Conditions

The Fiscal Year (FY) 2023 DHS Standard Terms and Conditions apply to all new federal financial assistance awards funded in FY 2023. These terms and conditions flow down to subrecipients unless an award term or condition specifically indicates otherwise. The United States has the right to seek judicial enforcement of these obligations.

All legislation and digital resources are referenced with no digital links. The FY 2023 DHS Standard Terms and Conditions will be housed on dhs.gov at www.dhs.gov/publication/fy15-dhs- standard-terms-and-conditions.

A. Assurances, Administrative Requirements, Cost Principles, Representations and Certifications

I. DHS financial assistance recipients must complete either the Office of Management and Budget (OMB) Standard Form 424B Assurances – NonConstruction Programs, or OMB Standard Form 424D Assurances – Construction Programs, as applicable. Certain assurances in these documents may not be applicable to your program, and the DHS financial assistance office (DHS FAO) may require applicants to certify additional assurances. Applicants are required to fill out the assurances as instructed by the awarding agency.

II. DHS financial assistance recipients are required to follow the applicable provisions of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards located at Title 2, Code of Federal Regulations (C.F.R.) Part 200 and adopted by DHS at 2 C.F.R. Part 3002. (SEE SPECIAL CONSIDERATIONS FOR STATES, LOCAL GOVERNMENTS AND INDIAN TRIBES BELOW)

III. By accepting this agreement, recipients, and their executives, as defined in 2 C.F.R. § 170.315, certify that their policies are in accordance with OMB's guidance located at 2 C.F.R. Part 200, all applicable federal laws, and relevant Executive guidance. (SEE CFR PART 200 § 200.317 PROCUREMENTS BY STATES BELOW)

B. General Acknowledgements and Assurances

All recipients, subrecipients, successors, transferees, and assignees must acknowledge and agree to comply with applicable provisions governing DHS access to records, accounts, documents, information, facilities, and staff.

I. Recipients must cooperate with any DHS compliance reviews or compliance investigations conducted by DHS.

II. Recipients must give DHS access to examine and copy records, accounts, and other documents and sources of information related to the federal financial assistance award and permit access to facilities or personnel.

III. Recipients must submit timely, complete, and accurate reports to the appropriate DHS officials and maintain appropriate backup documentation to support the reports.

IV. Recipients must comply with all other special reporting, data collection, and evaluation requirements, as prescribed by law, or detailed in program guidance.

V. Recipients (as defined in 2 C.F.R. Part 200 and including recipients acting as pass- through entities) of federal financial assistance from DHS or one of its awarding component agencies must complete the DHS Civil Rights Evaluation Tool within thirty (30) days of receipt of the Notice of Award for the first award under which this term applies. Recipients of multiple awards of DHS financial assistance should only submit one completed tool for their organization, not per award. After the initial submission, recipients are required to complete the tool once every two (2) years if they have an active award, not every time an

award is made. Recipients should submit the completed tool, including supporting materials, to CivilRightsEvaluation@hq.dhs.gov. This tool clarifies the civil rights obligations and related reporting requirements contained in the DHS Standard Terms and Conditions. Subrecipients are not required to complete and submit this tool to DHS. The evaluation tool can be found at https://www.dhs.gov/publication/dhs-civil-rights-evaluation-tool. DHS Civil Rights Evaluation Tool | Homeland Security

The DHS Office for Civil Rights and Civil Liberties will consider, in its discretion, granting an extension if the recipient identifies steps and a timeline for completing the tool. Recipients should request extensions by emailing the request to CivilRightsEvaluation@hq.dhs.gov prior to expiration of the 30-day deadline.

C. Standard Terms & Conditions

I Acknowledgement of Federal Funding from DHS

Recipients must acknowledge their use of federal funding when issuing statements, press releases, requests for proposal, bid invitations, and other documents describing projects or programs funded in whole or in part with federal funds.

II Activities Conducted Abroad

Recipients must ensure that project activities performed outside the United States are coordinated as necessary with appropriate government authorities and that appropriate licenses, permits, or approvals are obtained.

III Age Discrimination Act of 1975

Recipients must comply with the requirements of the Age Discrimination Act of 1975, Public Law 94-135 (1975) (codified as amended at Title 42, U.S. Code, § 6101 et seq.), which prohibits discrimination on the basis of age in any program or activity receiving federal financial assistance.

IV Americans with Disabilities Act of 1990

Recipients must comply with the requirements of Titles I, II, and III of the Americans with Disabilities Act, Pub. L. 101-336 (1990) (codified as amended at 42 U.S.C. §§ 12101– 12213), which prohibits recipients from discriminating on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities.

V Best Practices for Collection and Use of Personally Identifiable Information

Recipients who collect personally identifiable information (PII) are required to have a publicly available privacy policy that describes standards on the usage and maintenance of the PII they collect. DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. Recipients may also find the DHS Privacy Impact Assessments: Privacy Guidance and Privacy Template as useful resources respectively.

VI Civil Rights Act of 1964 – Title VI

Recipients must comply with the requirements of Title VI of the Civil Rights Act of 1964 (codified as amended at 42 U.S.C. § 2000d et seq.), which provides that no person in the United States will, on the grounds of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance. DHS implementing regulations for the Act are found at 6 C.F.R. Part 21 and 44 C.F.R. Part 7.

VII Civil Rights Act of 1968

Recipients must comply with Title VIII of the Civil Rights Act of 1968, Pub. L. 90-284, as amended through Pub. L. 113-4, which prohibits recipients from discriminating in the sale, rental, financing, and advertising of dwellings, or in the provision of services in connection therewith, on the basis of race, color, national

origin, religion, disability, familial status, and sex (see 42 U.S.C. § 3601 et seq.), as implemented by the U.S. Department of Housing and Urban Development at 24 C.F.R. Part 100. The prohibition on disability discrimination includes the requirement that new multifamily housing with four or more dwelling units—

i.e., the public and common use areas and individual apartment units (all units in buildings with elevators and ground-floor units in buildings without elevators)—be designed and constructed with certain accessible features. (See 24 C.F.R. Part 100, Subpart D.)

VIII Copyright

Recipients must affix the applicable copyright notices of 17 U.S.C. §§ 401 or 402 and an acknowledgement of U.S. Government sponsorship (including the award number) to any work first produced under federal financial assistance awards.

IX Debarment and Suspension

Recipients are subject to the non-procurement debarment and suspension regulations implementing Executive Orders (E.O.) 12549 and 12689, which are at 2 C.F.R. Part 180 as adopted by DHS at 2 C.F.R. Part 3002. These regulations restrict federal financial assistance awards, subawards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in federal assistance programs or activities.

X Drug-Free Workplace Regulations

Recipients must comply with drug-free workplace requirements in Subpart B (or Subpart C, if the recipient is an individual) of 2 C.F.R. Part 3001, which adopts the Government- wide implementation (2 C.F.R. Part 182) of Sec. 5152-5158 of the Drug-Free Workplace Act of 1988 (41 U.S.C. §§ 8101-8106).

XI Duplication of Benefits

Any cost allocable to a particular federal financial assistance award provided for in 2 C.F.R. Part 200, Subpart E may not be charged to other federal financial assistance awards to overcome fund deficiencies; to avoid restrictions imposed by federal statutes, regulations, or federal financial assistance award terms and conditions; or for other reasons. However, these prohibitions would not preclude recipients from shifting costs that are allowable under two or more awards in accordance with existing federal statutes, regulations, or the federal financial assistance award terms and conditions may not be charged to other federal financial assistance awards to overcome fund deficiencies; to avoid restrictions imposed by federal statutes, regulations, or federal financial assistance award terms and conditions; or for other reasons.

XII Education Amendments of 1972 (Equal Opportunity in Education Act) – Title IX

Recipients must comply with the requirements of Title IX of the Education Amendments of 1972, Pub. L. 92-318 (1972) (codified as amended at 20 U.S.C. § 1681 et seq.), which provide that no person in the United States will, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any educational program or activity receiving federal financial assistance. DHS implementing regulations are codified at 6 C.F.R. Part 17 and 44 C.F.R. Part 19.

XIII E.O. 14074 – Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety

Recipient State, Tribal, local, or territorial law enforcement agencies must comply with the requirements of section 12(c) of E.O. 14074. Recipient State, Tribal, local, or territorial law enforcement agencies are also encouraged to adopt and enforce policies consistent with E.O. 14074 to support safe and effective policing.

XIV Energy Policy and Conservation Act

Recipients must comply with the requirements of the Energy Policy and Conservation Act, Pub. L. 94- 163 (1975) (codified as amended at 42 U.S.C. § 6201 et seq.), which contain policies relating to energy efficiency that are defined in the state energy conservation plan issued in compliance with this Act.

XV False Claims Act and Program Fraud Civil Remedies

Recipients must comply with the requirements of the False Claims Act, 31 U.S.C. §§3729-3733, which prohibit the submission of false or fraudulent claims for payment to the Federal Government. (See 31 U.S.C. §§ 3801-3812, which details the administrative remedies for false claims and statements made.)

XVI Federal Debt Status

All recipients are required to be non-delinquent in their repayment of any federal debt. Examples of relevant debt include delinquent payroll and other taxes, audit disallowances, and benefit overpayments. (See OMB Circular A-129.)

XVII Federal Leadership on Reducing Text Messaging while Driving

Recipients are encouraged to adopt and enforce policies that ban text messaging while driving as described in E.O. 13513, including conducting initiatives described in Section 3(a) of the Order when on official government business or when performing any work for or on behalf of the Federal Government.

XVIII Fly America Act of 1974

Recipients must comply with Preference for U.S. Flag Air Carriers (air carriers holding certificates under 49 U.S.C.) for international air transportation of people and property to the extent that such service is available, in accordance with the International Air Transportation Fair Competitive Practices Act of 1974, 49 U.S.C. § 40118, and the interpretative guidelines issued by the Comptroller General of the United States in the March 31, 1981, amendment to Comptroller General Decision B-138942.

XIX Hotel and Motel Fire Safety Act of 1990

Recipients must ensure that all conference, meeting, convention, or training space funded in whole or in part with federal funds complies with the fire prevention and control guidelines of Section 6 of the Hotel and Motel Fire Safety Act of 1990, 15 U.S.C. § 2225a

XX John S. McCain National Defense Authorization Act of Fiscal Year 2019

Recipients, subrecipients, and their contractors and subcontractors are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to DHS recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

XXI Limited English Proficiency (Civil Rights Act of 1964, Title VI)

Recipients must comply with Title VI of the Civil Rights Act of 1964, (42 U.S.C. § 2000d et seq.) prohibition against discrimination on the basis of national origin, which requires that recipients of federal financial assistance take reasonable steps to provide meaningful access to persons with limited English proficiency (LEP) to their programs and services. For additional assistance and information regarding language access obligations, please refer to the DHS Recipient Guidance: https://www.dhs.gov/guidance- published-help- department- supported-organizations-provide-meaningful-access-people-limited and additional resources on http://www.lep.gov.

XXII Lobbying Prohibitions

Recipients must comply with 31 U.S.C. § 1352, which provides that none of the funds provided under a federal financial assistance award may be expended by the recipient to pay any person to influence, or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any federal action related to a federal award or contract, including any extension, continuation, renewal, amendment, or modification.

XXIII National Environmental Policy Act

Recipients must comply with the requirements of the National Environmental Policy Act of 1969, (NEPA) Pub. L. 91-190 (1970) (codified as amended at 42 U.S.C. § 4321 et seq. and the Council on Environmental Quality (CEQ) Regulations for Implementing the Procedural Provisions of NEPA, which require recipients to use all practicable means within their authority, and consistent with other essential considerations of national policy, to create and maintain conditions under which people and nature can exist in productive harmony and fulfill the social, economic, and other needs of present and future generations of Americans.

XXIV Nondiscrimination in Matters Pertaining to Faith-Based Organizations

It is DHS policy to ensure the equal treatment of faith-based organizations in social service programs administered or supported by DHS or its component agencies, enabling those organizations to participate in providing important social services to beneficiaries. Recipients must comply with the equal treatment policies and requirements contained in 6 C.F.R. Part 19 and other applicable statues, regulations, and guidance governing the participations of faith- based organizations in individual DHS programs.

XXV Non-Supplanting Requirement

Recipients receiving federal financial assistance awards made under programs that prohibit supplanting by law must ensure that federal funds do not replace (supplant) funds that have been budgeted for the same purpose through non-federal sources.

XXVI Notice of Funding Opportunity Requirements

All the instructions, guidance, limitations, and other conditions set forth in the Notice of Funding Opportunity (NOFO) for this program are incorporated here by reference in the award terms and conditions. All recipients must comply with any such requirements set forth in the program NOFO.

XXVII Patents and Intellectual Property Rights

Recipients are subject to the Bayh-Dole Act, 35 U.S.C. § 200 et seq, unless otherwise provided by law. Recipients are subject to the specific requirements governing the development, reporting, and disposition of rights to inventions and patents resulting from federal financial assistance awards located at 37 C.F.R. Part 401 and the standard patent rights clause located at 37 C.F.R. § 401.14.

XXVIII Procurement of Recovered Materials

States, political subdivisions of states, and their contractors must comply with Section 6002 of the Solid Waste Disposal Act, Pub. L. 89-272 (1965), (codified as amended by the Resource Conservation and Recovery Act, 42 U.S.C. § 6962.) The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 C.F.R. Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition.

XXIX Rehabilitation Act of 1973

Recipients must comply with the requirements of Section 504 of the Rehabilitation Act of 1973, Pub. L. 93-112 (1973), (codified as amended at 29 U.S.C. § 794,) which provides that no otherwise qualified handicapped individuals in the United States will, solely by reason of the handicap, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance.

XXX Reporting of Matters Related to Recipient Integrity and Performance

General Reporting Requirements:

If the total value of any currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies exceeds $10,000,000 for any period of time during the period of performance of this federal award, then the recipients must comply with the requirements set forth in the government-wide Award Term and Condition for Recipient Integrity and Performance Matters located at 2

C.F.R. Part 200, Appendix XII, the full text of which is incorporated here by reference in the award terms and conditions.

XXXI Reporting Subawards and Executive Compensation

Reporting of first tier subawards.

Recipients are required to comply with the requirements set forth in the government-wide award term on Reporting Subawards and Executive Compensation located at 2 C.F.R. Part 170, Appendix A, the full text of which is incorporated here by reference in the award terms and conditions.

XXXII Required Use of American Iron, Steel, Manufactured Products, and Construction Materials

Recipients must comply with the "Build America, Buy America" provisions of the Infrastructure Investment and Jobs Act and E.O. 14005. Recipients of an award of Federal financial assistance from a program for infrastructure are hereby notified that none of the funds provided under this award may be used for a project for infrastructure unless:

(1) all iron and steel used in the project are produced in the United States--this means all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States;
(2) all manufactured products used in the project are produced in the United States—this means the manufactured product was manufactured in the United States; and the cost of the components of the manufactured product that are mined, produced, or manufactured in the United States is greater than 55 percent of the total cost of all components of the manufactured product, unless another standard for determining the minimum amount of domestic content of the manufactured product has been established under applicable law or regulation; and
(3) all construction materials are manufactured in the United States—this means that all manufacturing processes for the construction material occurred in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

Waivers

When necessary, recipients may apply for, and the agency may grant, a waiver from these requirements. Information on the process for requesting a waiver from these requirements is on the website below.

(a) When the Federal agency has made a determination that one of the following exceptions applies, the awarding official may waive the application of the domestic content procurement preference in any case in which the agency determines that:
(1) applying the domestic content procurement preference would be inconsistent with the public interest;
(2) the types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality; or
(3) the inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25 percent.

A request to waive the application of the domestic content procurement preference must be in writing. The agency will provide instructions on the format, contents, and supporting materials required for any waiver request. Waiver requests are subject to public comment periods of no less than 15 days and must be reviewed by the Made in America Office.

There may be instances where an award qualifies, in whole or in part, for an existing waiver described at "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure FEMA.gov.

The awarding Component may provide specific instructions to Recipients of awards from infrastructure programs that are subject to the "Build America, Buy America" provisions. Recipients should refer to the Notice of Funding Opportunity for further information on the Buy America preference and waiver process.

XXXIII SAFECOM

Recipients receiving federal financial assistance awards made under programs that provide emergency communication equipment and its related activities must comply with the SAFECOM Guidance for Emergency Communication Grants, including provisions on technical standards that ensure and enhance interoperable communications.

XXXIV Terrorist Financing

Recipients must comply with E.O. 13224 and U.S. laws that prohibit transactions with, and the provisions of resources and support to, individuals and organizations associated with terrorism. Recipients are legally responsible to ensure compliance with the Order and laws.

XXXV Trafficking Victims Protection Act of 2000 (TVPA)

Trafficking in Persons.

Recipients must comply with the requirements of the government-wide financial assistance award term which implements Section 106 (g) of the Trafficking Victims Protection Act of 2000 (TVPA), codified as amended at 22 U.S.C. § 7104. The award term is located at 2 C.F.R. § 175.15, the full text of which is incorporated here by reference.

XXXVI Universal Identifier and System of Award Management

Requirements for System for Award Management and Unique Entity Identifier Recipients are required to comply with the requirements set forth in the government-wide financial assistance award term regarding the System for Award Management and Universal Identifier Requirements located at 2 C.F.R. Part 25, Appendix A, the full text of which is incorporated here by reference.

XXXVII USA PATRIOT Act of 2001

Recipients must comply with requirements of Section 817 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which amends 18 U.S.C. §§ 175–175c.

XXXVIII Use of DHS Seal, Logo and Flags

Recipients must obtain permission from their DHS FAO prior to using the DHS seal(s), logos, crests or reproductions of flags or likenesses of DHS agency officials, including use of the United States Coast Guard seal, logo, crests or reproductions of flags or likenesses of Coast Guard officials.

XXXIX Whistleblower Protection Act

Recipients must comply with the statutory requirements for whistleblower protections (if applicable) at 10 U.S.C § 2409, 41 U.S.C. § 4712, and 10 U.S.C. § 2324, 41 U.S.C. §§ 4304 and 4310