AZDOHS Cyber Readiness Program FAQs

General

- Who do I contact to learn more?
    - Please email CyberReadinessSupport@azdohs.gov for any inquiries or concerns.

- How much will this cost my organization? What is the cost of the cyber readiness program?
    - Nothing. The State of Arizona has funded this program with recurring general fund dollars. Additionally, grants provided by the US Department of Homeland Security are available to support this program. There is no cost to the participating local organizations. Participating organizations will not be asked to pay for future use of the products.

- How many licenses are available?
    - Licenses are provided based on the amount requested through application. Though there is no max, however, this amount is a realistic amount based on organization size. The number of licenses will be reassessed during deployment status reviews.

- What will be required of local and tribal applicant organizations?
    - Applicant organizations are required to have support from organization executives and provide an executive and technical point of contact. Applicant organizations are required to make consistent progress with onboarding and use of the product(s) at their organizations. Licenses assigned to non-responsive organizations may be re-allocated to another organization.

- How much time does it take to set these products up in my environment?
    - Time to setup will vary with each product. The program's vendor partners, and the State's internal product owners will work with your technical team on the setup(s). The intent of this program is to provide support to your organization to make the onboarding process as minimal as possible. Professional assistance will be provided from the vendors to assist you throughout.

- Who do I contact for support?
    - CyberReadinessSupport@azdohs.gov will be your first point of contact. Please contact the vendor partner directly for product specific support. Their contact information is located in your onboarding guide.

- What happens after the 12 month performance period?
    - Funding for these licenses are provided by State general fund money. The Arizona Department of Homeland Security is monitoring performance and utilization of each tool. Homeland Security is prioritizing cyber security and this is the fourth year of program expansion. Additionally, the governance committee (Cyber Readiness Task Force) will be reviewing and making recommendations about future expansion.
- What products are available?
    - Multi-Factor Authentication (MFA)
        - Thales
    - Advanced Endpoint Protection (AEP)
        - Crowdstrike
    - Converged Endpoint Management (XEM)
        - Tanium
    - Web App Firewall (WAF)
        - Cloudflare
    - Security Awareness Training (SAT)
        - Infosec IQ

- How are the products hosted?
    - All five products are vendor hosted in a Software as a Service (SaaS) model. Some configuration and software installation at your organization will be required.

- How and why were these specific products chosen?
    - The AZDOHS Cyber Command is a member of the multi-agency State Enterprise Security Program Advisory Council (ESPAC.AZ.Gov). One of ESPAC's responsibilities is to work with State agencies to select cybersecurity products for purchase and deployment to 80+ different State government agencies at no

additional cost to them. ESPAC reviews security gaps based on the CIS Top 18, and looks for ways to close the greatest number of gaps for the greatest number of entities. State agencies, working together, developed technical requirements, evaluated products, and completed a selection and procurement process that meets the requirements of the program. A team of Local government representatives, along with the State, selected the same products implemented by the State which will similarly be deployed to Arizona local and tribal governments. AZDOHS Cyber Command has significant experience deploying these specific products to 80+ different organizations. Additionally, the grant program realizes significantly reduced pricing (economies of scale) using the same products as the State and can benefit from the State's deployment experiences and continuous improvement.

- What is the application process?
    - If you have never applied to the program, please fill out the application request form (linked here). Your application will be reviewed by our team and we will issue an award if the application is complete and your organization is eligible. You will receive information on what products you have been awarded and next steps to begin your deployments.

- My organization participated in the grant program in previous years. Do I need to re-apply?
    - No, at this time we are not requiring a new application to be submitted to continue use of the previously awarded products. If you would like to apply for additional products after your initial application, please email CyberReadinessSupport@azdohs.gov.

- If we apply do we have to use all of the products and all of the features offered?
    - No, these products are available carte blanche. It is up to your discretion if you apply for one, multiple, or all of the products offered to best suit the needs of your organization. All features within the products do not need to be utilized either.

- What if we have other features we'd like to use for a product that is not included in the program offering?
    - We have identified with each vendor what additional features are available to be purchased outside of the program for their product. These additions would not be paid for through the program and would need to be paid for through your organization's budget. If you decide to purchase additional features, please let us know by emailing CyberReadinessSupport@azdohs.gov so the Cyber Readiness Task Force can be made aware to determine if new features can be included in future purchases as part of the Program.

- How do we apply for a product we didn't ask for as part of our original application?
  - Please do not submit a new application request form. Email CyberReadinessSupport@azdohs.gov indicating your interest in adding a new product to your original award. We may request additional information depending on which product you are looking to add. We will then update your original application on the back end to reflect the new award.

- Can we request additional licenses after being awarded?
  - Yes, please email CyberReadinessSupport@azdohs.gov indicating which products you would like to increase licenses for and how many you need.

- Why should our organization join the program?
  - The Arizona Department of Homeland Security purchased the tool licenses in order to achieve greater visibility, efficiency, and cost savings. By purchasing the licenses on behalf of all of the participants, the State was able to negotiate economies of scale discounts on the license cost. In addition, some of these tools have thresholds for customer size and are not able to sell below a specific number.
    By participating in the Cyber Readiness Program your organization can benefit from the cost savings by not having to purchase products through your own budget, as well as the increased cybersecurity posture provided by these tools if you don't already have something in place.

- How do we know if our organization is eligible?
  - "Local government" is defined in 6 U.S.C. § 101(13) as:
    - A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;
    - An Indian tribe or authorized tribal organization; and
    - A rural community, unincorporated town or village, or other public entity.

- If we were awarded licenses, when do we have to have them deployed by?
  - The licenses awarded are yours to deploy on a timeline of your choosing. We understand not everything can be done at once and it takes time and resources to get these things done. We just ask that if you decide at any point not to utilize a product, or choose to deploy to your full environment please let us know so we can reallocate the unused licenses. We may check in from time to time to confirm with entities that haven't deployed that they still intend to do so, but there isn't any pressure from our side that it has to be done within x period of time.

- Can we use a managed service Provider (MSP)?
    - Yes, you can allow access to an MSP to the products you have been awarded. Please note, an individual from your organization must apply, an MSP cannot apply on your behalf.
    -
- How long will this program continue for?
    - Funding for these licenses are provided by State on-going general fund money and expected to continue long term.

- How do I change the contacts for my organization?
    - Follow the steps provided on this link:
        - https://app.smartsheet.com/b/form/43eefcdb093244169ed032071eaf1d11

Advanced Endpoint Protection (AEP)

- What is Advanced Endpoint Protection?
    - Advanced Endpoint Protection. For organizations struggling with the ineffectiveness and complexity of legacy antivirus solutions, the product is a complete AV replacement solution. This product delivers superior protection with a single lightweight agent that does not require constant updates.

- What is required to install the AEP agent?
    - You will receive console access after initial configuration. In the console, there are multiple resources and articles to assist you on everything from installation to tuning.

- How do I get Support? (in general section)
    - CyberReadinessSupport@azdohs.gov will be your first point of contact. Please contact the service partner directly for product specific support. Their contact information is located in your onboarding guide.

- What level of access will I have?
    - There are multiple levels of access which your agency or your liaison can manage on behalf of your agency. These range from full administrator access to read-only and roles somewhere in between.

- Is USB device policy included?
    - Yes

Multi-Factor Authentication (MFA)

- What is MFA?
  - Multi-factor authentication is an electronic authentication method in which a user is granted access to a website, application, operating system or other resource only after successfully presenting two or more pieces of evidence to an authentication mechanism:
    - Knowledge – something you know (static password or PIN)
    - Possession – something you have (token or mobile device)
    - Inherence – something you are (biometric scan, finger, face, retina, voice)

- Why use MFA?
  - By requiring multiple forms of authentication, the risk of compromise of any single authentication credential is significantly mitigated. Knowledge-based credentials such as static passwords are highly vulnerable to guessing, phishing and brute force attacks. If authentication is limited to password credentials, the organization is highly vulnerable to attacks such as ransomware and other cyber-crimes. According to the National Institute of Standards and Technology, requiring additional authentication factors reduces the risk to near zero.

- Does STA MFA integrate with existing user repositories?
  - STA significantly reduces the administrative burden of user lifecycle management by synchronizing user identities with user details contained in existing user repositories supporting LDAP or SQL. Most often, customers synchronize from their on-premises AD. User basic management takes place in ADUC; the Safenet Sync Agent, replicates a subset of the user data with STA based on user group inclusions within AD.

- Is MFA limited to administrator access?
  - STA MFA is available for privileged and unprivileged users. Privileged users, such as IT Administrators, have the greatest access to confidential resources and data. For this reason and a variety of other good reasons, the privileged users should be the first adopters for MFA. Unprivileged users often have access to some confidential resources and data and should be included in the longer term MFA requirement. Cyber insurance requirements dictate that all users accessing the internal network use MFA. NOTE for Schools: At this time, students are not covered by the Cybersecurity Readiness Program.

- Which authentication factors are available for MFA?

- Software tokens running on Mobile Platforms are the preferred authenticator. Hardware tokens are available free of charge. A pattern matching, zero-foot print authenticator called GrIDsure is available free of charge. SMS/Voice delivery authenticators are available free of charge, but may incur a separate per message fee. SMTP delivery authenticators are available free of charge.

- What resources can be protected?
  - STA is more than an MFA product; it is Identity as a Service (IDaaS) with a fully featured Identity and Access Management product. It can protect thousands of on-premises, extra-net and internet resources using standards-based authentication protocols and agents as required.

- How do I get Support? (in general section)
  - CyberReadinessSupport@azdohs.gov will be your first point of contact. Please contact the service partner directly for product specific support. Their contact information is located in your onboarding guide.

Security Awareness Training (SAT)/Anti-phishing

- What is SAT?
  - Security Awareness Training
    - Security awareness training involves providing cybersecurity education to employees about a variety of threats to information security and technology and policies and procedures for addressing them.
  - Anti-Phishing
    - Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords or credit card details, by disguising itself as a trustworthy entity in an electronic communication.
      - Anti-phishing training will teach employees how to spot potential phishing emails and how to report them.

- How do I get Support? (General section)
  - CyberReadinessSupport@azdohs.gov will be your first point of contact. Please contact the service partner directly for product specific support. Their contact information is located in your onboarding guide.

- Are participating organizations required to have a .Gov email address?
  - Participants are not required to have .Gov email addresses but they are required to have their own unique top level domain. Shared domains, like those provided by Internet Service Providers (Cox.net, CenturyLink.net, etc.), cannot be used.

- We highly recommend all government organizations consider using .Gov top level domains for communicating and providing services to citizens. You can find more information here:
  - https://aset.az.gov/service/online-services/domain-name-approval
  - https://home.dotgov.gov/registration/requirements/

Web Application Firewall (WAF)

- What is a Web Application Firewall?
  - WAF acts as a shield between your websites and potential users, protecting sites from common vulnerabilities, botnets, Denial of Service (DDoS), and other attacks originating from the Internet. It can be run in the default state, or customized to suit specific security requirements.

- What services am I able to protect with WAF?
  - By default, any website available on the Internet using port 80 (HTTP) and/or port 443 (HTTPS). You can also protect traffic on other ports by using Cloudflare Spectrum, included in the program.

- What is DDoS mitigation?
  - DDoS mitigation refers to the process of successfully protecting a targeted server or network from a distributed denial-of-service (DDoS) attack, through both automated and manual intervention.
  - A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the operations of server, service or network by overwhelming the target or its surrounding infrastructure. A common example is a flood of internet traffic.

- What level of access will I have?
  - There are multiple levels of access which your agency or your liaison can manage on behalf of your agency. These range from full administrator access to read-only, with roles that can also be scoped to specific to dashboard features. Within the organization's main tenant, access can also be provided on a domain basis.

- How much time will a WAF take to set up?
  - Once your domain is activated through the DNS setup process, the WAF takes about 15 minutes to configure and enable. It can be enabled in a logging mode first if users are interested in reviewing data before moving to an active, blocking state.

- Do my websites need to be hosted locally?

  - WAF works no matter where your websites are hosted, as long as they are publicly accessible.

- How do I get Support? (in general section)
  - CyberReadinessSupport@azdohs.gov will be your first point of contact. Please contact the service partner directly for product specific support. Their contact information is located in your onboarding guide.

Converged Endpoint Management (XEM)

- What is XEM?
  - Numerous government organizations trust XEM Converged Endpoint Management platform to provide unrivaled access to real-time asset visibility and the ability to patch at scale with certainty (including devices that are on or off network or VPN).

- What's needed to deploy the XEM agent?
  - You can use many different options to deploy XEM. Any software deployment tool can be used to deploy the agent.

- Why should we use XEM?
  - XEM brings IT Operations, Security and Risk Management teams together – with a single platform for complete visibility, control and trust in IT decision-making.

- Why do we need to open the firewall ports?
  - XEM is a SaaS solution that requires access to the network.

- What does XEM do for me?
  - You can use XEM to gain valuable visibility and control of your assets in real time. You can take real time actions with the real time information. You can also use XEM to manage patching in your environment - both OS and 3rd party.

- Why do you need my Identity provider?
  - Because XEM is a SaaS solution, it is necessary to protect access to the console and validate the identity of a user.

- How do I get Support? (in general section)
  - CyberReadinessSupport@azdohs.gov will be your first point of contact. Please contact the service partner directly for product specific support. Their contact information is located in your onboarding guide.

- Can Arizona Department of Homeland Security (AZDOHS) see my data?
    - AZDOHS is not authorized to view or manipulate any endpoint data of any participant for any reason. Should you request assistance that may require AZDOHS pushing actions on your machines it will not be done so without expressed written permission. If you have additional questions please contact AZDOHS at cyberreadinesssupport@azdohs.gov.

- Can I add additional modules through the program?
    - We have identified with each vendor what additional features are available to be purchased outside of the program for their product. These additions would not be paid for through the program and would need to be paid for through your organization's budget. If you decide to purchase additional features, please let us know by emailing CyberReadinessSupport@azdohs.gov so the Cyber Readiness Task Force can be made aware to determine if new features can be included in future purchases as part of the Program.

- How do I recommend future products to be included in the program?
    - Please email CyberReadinessSupport@azdohs.gov letting the team know what features or products you'd like to see included. The team will discuss with the Cyber Readiness Program Task Force to see if future enhancements can be made.

- Is it too late to submit an application for the grant program?
    - xxx

- What is the State and Local Cyber Grant Content form for?
    - xxx

- How can I request a Project Manager to help us?
    - Please send all questions and concerns to cyberreadinesssupport@azdohs.gov.

- How do I know what products I was awarded?
    - Please send all questions and concerns to cyberreadinesssupport@azdohs.gov.