ARIZONA
DEPARTMENT OF ADMINISTRATION
TECHNOLOGY

NASCIO 2022 State IT Recognition Awards
Cybersecurity

Cyber Grant for Local and Tribal Governments in Arizona

Title: Cyber Grant for Local and Tribal Governments in Arizona
Category: Cybersecurity
State: Arizona
Contact: Bryan Beach
Bryan.Beach@azdoa.gov
(602) 316-8369
Start date: 9/2021
End date: ONGOING

EXECUTIVE SUMMARY

Situation

Arizona Governor Doug Ducey has publicly declared that cybersecurity is homeland security. To ensure that sensitive data and systems are adequately protected, the State of Arizona takes a multi-tiered approach by using best-of-breed cybersecurity tools and providing education and training to all state employees, ensuring the presence of both a technical and human firewall that can block many cyber attacks from being successful. Additionally, collaboration within the state fosters agency participation in enterprise-level decision making, partnerships with state, local, tribal, and territorial (SLTT) government entities, information sharing, and statewide strategy implementation.

Within the State of Arizona, it is especially vital that the personal information of its citizens be protected at all times, and critical services remain available. To build this layer of protection and gain the trust and confidence of citizens, the use of sophisticated cybersecurity tools and the capabilities provided by well-trained employees are absolute necessities at all levels of government.

The Enterprise Security Program Advisory Council (ESPAC) exists to actively collaborate with all levels of government to ensure that cybersecurity programs are developed and maintained effectively to keep pace with evolving threats. Moreover, Governor Ducey created the Arizona Cybersecurity Team that subsequently published a comprehensive list of recommendations to protect Arizona against cyber threats, including enhanced information sharing and collaboration efforts throughout the State.

Problems

Many local and tribal governments have gaps in their cybersecurity programs because they do not have the resources, knowledge, or the budget to purchase and install sufficient cybersecurity tools that protect their data and their networks from compromise. Many of these systems interconnect to each other, making the need to protect systems at all levels of government essential.

Solution

To better prepare and equip less-resourced local and tribal governments, a cyber grant program enables dedicated funding to provide multiple cybersecurity solutions that more effectively protect against threats in the cyber landscape.

CONCEPT

Through a cyber grant award from the Arizona Department of Homeland Security and the US Department of Homeland Security, local and tribal governments in Arizona who apply are able to obtain available cybersecurity tools through statewide contracts to keep their systems and data safe from bad actors attempting to identify and exploit possible vulnerabilities.

Key performance indicators include:

- Data Quality: Increased data collection and quality
- Cost Reduction: Easier system development and maintenance
- Increased Collaboration: Data exchanges with external systems
- Modular Design: More flexible and adaptive to allow for future changes
- Follows IT Standard: Promotes efficient, economical, and effective development
- Shareable: Capable of being shared and reused by other states, tribes, and agencies

SIGNIFICANCE

Using the US Department of Homeland Security grant to provide local governments with tools to fill cybersecurity gaps within their environments continues to be an innovative concept. It allows smaller and budget-constrained entities across Arizona to have access to some of the best-in-class technical solutions available in the marketplace.

Cybersecurity tools available to Arizona local and tribal governments, through this grant program include:

- Advanced Endpoint Protection (AEP) - Next-generation antivirus protection that leverages artificial intelligence and machine learning to identify malware before it executes.
- Anti-Phishing / Security Awareness Training (SAT) -
    - Anti-Phishing Training provides employees with examples of how to spot phishing attempts and suspicious emails requesting sensitive information from users or infecting systems with malware. This includes sending emails to employees with fake links, mimicking real phishing attempts from outside threats.

Employees who click on simulated links will be prompted to complete Security Awareness Training.

    - Security Awareness Training (SAT) features user-friendly online training courses that cover the latest cybersecurity best practices to educate employees on how to keep data and devices safe.

- Multi-Factor Authentication (MFA) - A security system that requires more than one method of authentication to verify a user's identity for a login or other transaction. MFA provides an extra layer of security to prevent unauthorized access to systems.
- Web Application Firewall (WAF) - An application firewall for HTTP applications. It applies a set of policies to help protect web applications from common web exploits that could affect an application's availability and compromise data.

IMPACT

Currently in its third year, 50+ local and tribal governments have participated in the cyber grant program awarded to the Arizona Department of Homeland Security in partnership with ESPAC to leverage the buying power, statewide contracts, and expertise of the Enterprise Security Team and the multi-jurisdictional volunteer liaison team. The state will continue to apply for the grant on a yearly basis to maintain cybersecurity resources for existing local and tribal governments while prioritizing new applicants to the grant program.

For more information, visit the Cyber Resources for Local and Tribal Governments page.