Vision:
To be the nationwide best practice for grant management and administration as well as a premier leader in cybersecurity among all state homeland security departments.

Mission:
Protect Arizona by providing strategic direction and access to resources that will enable all of the State's homeland security stakeholders to achieve our collective goals of: preventing terrorist attacks; enhancing border security; heightening cybersecurity efforts; reducing our vulnerability to all critical hazards; enhancing the capacity and expertise to plan for, mitigate, respond to and recover from all critical hazards that affect the safety, well-being, and economic security of Arizona; and building the resiliency of Arizona.

Agency Description:
The Department administers federal grants to State and local agencies to protect our border and prevent or reduce Arizona's vulnerability to terrorist attacks, as well as, driving best-in-class, enterprise cybersecurity solutions in an effort to ensure the protection of all government functions within the State of Arizona

Executive Summary:
The focus of the Department for Fiscal Year 2024 will be: to comply with all grant guidelines including obligating funds within 45 days of receipt of the 2023 grant award and monitoring subrecipients to ensure their compliance with grant guidelines; assist in identifying resources that can be used and shared statewide to strengthen the ability to work together to address common threats and vulnerabilities across the state; enhance public safety improve enterprise efficiencies, and enhance the overall cybersecurity, privacy, and resiliency of all data and systems throughout the State through statewide collaboration and leveraging partnerships.

The Department will increase efficiency by exploring automated systems, analyzing reimbursement data and engaging with stakeholders to minimize the amount of days to process completed reimbursements.

Summary of Multi-Year Strategic Priorities

#	Five Year Strategy	Start Year	Progress / Successes
1	Effectively manage homeland security grant funds	2017 (REV 2023)	• Operation Stonegarden Grants have funded **725,588.50** hours of law enforcement overtime, **249,092** vehicle stops, and **7877** apprehensions in an effort to secure our border • AZDOHS has monitored **1,695** subrecipient projects through site visits and desk reviews to ensure **100%** compliance on grant awards • Monitoring and oversight of grant funding has ensured over **99%** of grant funding is utilized
2	Build the statewide capacity to defend against and respond to cyber attacks	2021	• Moved the Enterprise Security Team to Arizona Department Of Homeland Security (AZDOHS) and opening of the Cyber Command Center at the Arizona Counter Terrorism Information Center (ACTIC) in 2021 • Expansion of Statewide Cyber Readiness Program to serve **222** local government entities, K-12 school districts, and tribal nations providing • The Arizona-Information Sharing Analysis Center (AZ-ISAC) now bringing together over **570** members from cities, counties, K-12 school districts, state agencies, federal partners, other states to share cyber information • All **15** counties were collaborating and communicating with each other though AZ-ISAC and shared communication platform during 2022 Elections • Coordinated incident response efforts through AZ-ISAC and shared communication platform when email systems were compromised
3	Create a more efficient Department	2017 (REV 2023)	• Engaged our stakeholders on a 1-on-1 basis to ensure education and mentorship occurs • Conducted stakeholder seminars to improve the reimbursement process • Conducted outreach and updated website to provide current policies and procedures • Decreased the AZDOHS average reimbursement processing time from 42 to **8.93** calendar days, in order to minimize stakeholder capital outlay (**79% reduction**)
4	Develop the Cybersecurity workforce	2024	• Five cybersecurity interns hired within AZDOHS and more across the state agencies • Meeting with community colleges and the Universities to discuss curriculum and workforce development initiatives • Participate in the Phoenix Chamber Foundation Workforce Development Collaborative

Strategy #	FY24 Annual Objectives	Objective Metrics	Annual Initiatives
#1	Maintain compliance with federal grant guidance	• Percent compliance with federal grant mandates • Number of projects monitored	• Reallocate funding from projects that do not expend their awarded amount to other projects that need funding to further support the homeland security mission • Ensure the success of Operation Stonegarden by conducting integrated planning team meetings and monitor key statistics such as: vehicle stops, overtime hours worked, and illegal aliens apprehended • Complete Sunset Review in fall 2023
#2	Continue to develop the capability to defend against and respond to cyber attacks across the State of Arizona	• State Agencies maintain a cybersecurity risk score of 725 or greater • # of agency risk assessments completed • % of enterprise security tool deployment and utilization • # of IOC's shared with SLTT partners • # of participants in the Statewide Cyber Readiness Program	• Increase enterprise cybersecurity tool adoption and maturity within the State Agencies • Continue deployment of cyber tools through the Statewide Cyber Readiness Program, specifically targeting K-12 schools • Continue to mature AZ-ISAC processes, governance, and grow membership • Review and revitalize ESPAC membership and processes • Support DEMA and ADOA initiatives to improve cybersecurity of the State
#3	Reduce days to reimburse stakeholders **(breakthrough)** Increase standard work for routine/frequent documents	• Average number of days to process completed reimbursement requests **(breakthrough)** • Number of improved AMS standard work processes	• Continuously seek ways to improve our internal processes • Engage with stakeholders on a 1-on-1 basis • Continuously collect and analyze data to determine reasons for delays • Explore automated systems to enhance grant related processes • Review business related functions and determine areas where policies and procedures can be revised, improved or re-written using standard work
#4	Explore ways to develop and provide workforce opportunities for K-12, 2YR, 4YR and non-traditional students	• # of attendees at hosted events • # of events hosted • # of student attendees • # of volunteers • # of community partners attendees • # of higher education institutions exhibitors	• Continuously build the cybersecurity ecosystem with education and community partners to increase number of individuals entering the cybersecurity workforce • Launch Girls in Cyber Event for middle and high school girls as a workforce development initiative to increase number of girls and women in cybersecurity • Conduct tabletop exercises with high school and college students • Collaborate with Community Colleges and Universities on Workforce Development efforts and Regional cybersecurity support

Arizona Cybersecurity Program Components
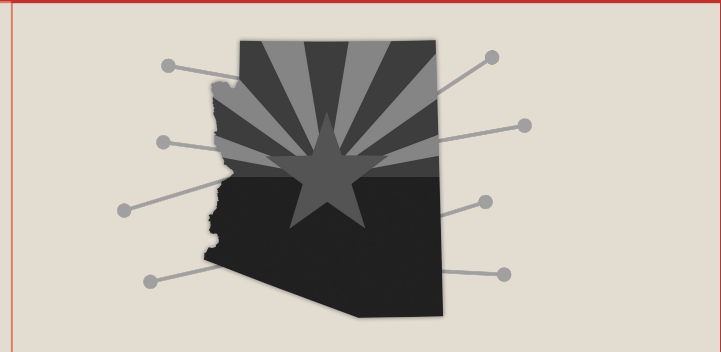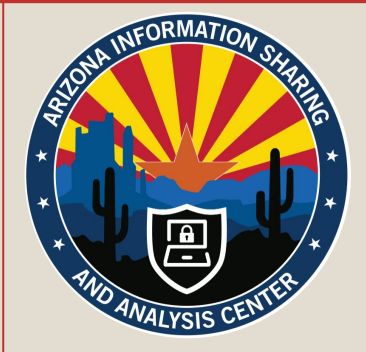
Cyber Command	AZ-ISAC	Cyber Joint Task Force	Statewide Cyber Readiness Program
Statewide Security Operations Center Statewide security and privacy policies/standards Enterprise Cybersecurity Tools Support Program Management	Statewide Perspective Fusion Center Integration (ACTIC) Threat Intelligence Platform Slack Workspace Monthly Threat Briefing and Newsletter DEMA Cyber Joint Task Force Coordination Collaboration with Federal partners	Penetration testing & vulnerability assessments Defensive strategy development and implementation Participation in national and state training exercises Information and intelligence sharing across the whole of government Provide post-attack cyber incident response, forensic analysis and recovery assistance to state and local agencies Develop cyber aptitude tests and skills training, threat identification methods and procedures Conduct Defensive Cyber operations for State agencies and critical infrastructure partners	Provide State Enterprise cybersecurity tools to SLTT and K-12 Schools • Anti-Phishing / Security Awareness Training (SAT) • Advanced Endpoint Protection (AEP) • Multi-Factor Authentication (MFA) • Web Application Firewall (WAF) • Converged Endpoint Management (XEM) • Security Assessments