Memorandum of Understanding
Between
The State of Arizona Department of Emergency and Military Affairs-Arizona National Guard
And
The County of Cochise, Arizona (also referred to as "Agency")

EXHIBIT A

Support provided to Agency under this Annex are broken down as follows:

Activity	Included activities	Type	# Personnel	Time
Threat Hunting		on-site/remote	3-5	5 days min.
	Computer vulnerability scans			
	Network device vulnerability scans			
	Network traffic packet capture			
	Host enumeration / identification			
	In-depth hunt for malicious code or network activity			
External Threat Posture Scanning		On-site/remote	1-2	1 day
	Scan for unsecured Internet-facing ports			
	Domain Name System configuration validation (data leak)			
	Web server API mis-configuration (data leak)			
Web Application Scanning		remote	1-2	1 day
	Standard external web application vulnerability assessment			
Log analysis		remote	1	2-3 days
- Windows event logs	Correlation of log events with known malicious activity			
- Firewall Logs	from open source threat intel sources			
- Web or other server logs				
Malware Reverse Engineering/Analysis		remote	1	2 days min.
	Forensic analysis of malware sample			
	Dynamic and static analysis			
	Provide Indicators of compromise (IOCs) back to agency			
Evaluate and Assist		on-site	1	1 day
	On-site visit to determine scope and nature of cyber threat			

If an official request is made for the AZNG Cyber JTF to respond to an incident, all activities listed above are within scope of that response. Any CJTF Team response will require 3-5 personnel for a minimum of 5 days, not all personnel or activities occurring at the requesting agency location. Agencies may request one or more of the above activities independent of a team response; however, such requests will be actioned within the limits of team commitments and available resources.