CYBER SHARING MATURITY MODEL

		Sharing Capabilities			Resources
	Level	Score – Limited (1)	Score – Progressing (2)	Score – Optimizing (3)	
1	**Cyber Threat Awareness**	- Signed up for news feeds. - Email lists.	- RSS feeds to applications (i.e., Slack) - Member of an ISAC/ISAO.	- Direct feeds to security tools (i.e., APIs for automatic feeds)	• DHS Cyber Information Sharing and Collaboration Program (CISCP) • DHS Enhanced Cybersecurity Services (ECS) • **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**
2	**Cyber Threat Detection and Recognition**	- Some Manual processes in place for generating alerts.	- Hybrid alerting – Basic automatic and some manual processes in place.	- Some Automated detection and alerting - Some Automated integrations from servers to endpoints. - Automated malicious IP address blocking.	• US-CERT Alerts • DHS Cyber Information Sharing and Collaboration Program (CISCP) • DHS Enhanced Cybersecurity Services (ECS) • Multi-State Information Sharing & Analysis Center
3	**Internal Cyber Threat Sharing**	- Generic policies and procedures for sharing of threat data to internal sources. - Limited sharing from InfoSec to IT teams.	- Hybrid alerting – automatic and manual processes for sharing data to the work force.	- Mostly following fully-automated processes for sharing threat data to the workforce. - Mostly integrated communications between IT and InfoSec teams.	• National Preparedness Course Catalog ○ AWR-177-W Information Risk Management ○ AWR-353-W Using the Community Cyber Security Maturity Model (CCSMM) to Develop a Cyber Security Program
4	**Membership in Cyber Sharing Networks**	- Free tier membership with an ISAC/ISAO.	- Paid membership with ISAC/ISAO - Limited technical connections with the ISAC/ISAO.	- Fully automated connections with the ISAO. - The workforce is active in the ISAC/ISAO.	• ISAO Standards Org - Information Sharing Groups • DHS Cyber Information Sharing and Collaboration Program (CISCP)
5	**Intake Information Shared by Cyber Sharing Network**	- Some automated processes and connections.	- Most connections are integrated with an ISAO or business partners.	- All automated sharing activities are focused on customizing alerts and maintaining connections.	• ISAO Standards Organization: *ISAO 300-1 Introduction to Information Sharing*, Section 3.2 Applying Shared Information • ISAO Standards Organization: *ISAO 300-1 Introduction to Information Sharing*, Figure 3. Applying Information to Cybersecurity Risks