THE CJIS SECURITY POLICY AND CENTRALIZATION OF VENDOR REQUIREMENTS

What Are Other States Doing?

by William M. Tatun

Having been a state CJIS Systems Officer (CSO) and the person responsible for managing the security of the CJIS systems through implementing and ensuring compliance with CJIS Security Policy, I truly understand the complexities involved with trying to adequately address all the CJIS-related vendor requirements. I have lived through the myriad of vendor emails, calls and visits to the office all desperately looking for efficient ways to deal with all the requirements. All of them telling me how having to go through a fingerprint background check for every customer agency (which in some cases was 100s of agencies) in my state seemed archaic and inefficient and hoping for a better way.

Sound too familiar? Were they far off in their assessment?

Well, I have good news. There are better ways and there are states that have implemented progressive processes to streamline and centralize certain CJIS requirements at the state level affording them many benefits to include, but not be limited to, increases in efficiency, quality assurance and overall security compliance.

Let's look at some of the CJIS Security Policy requirements that apply to all vendors. There are five specific CJIS policy compliance areas that have been identified as a "good-fit" for state level centralization and coordination. They are:

- Personnel Screening (background checks)
- Audit (of solution)
- the CJIS Security Addendum
- Incident Response
- Security Awareness Training

States that have implemented programs and processes to centralize and coordinate one or all of the above requirements have been able to recognize real-life benefits and better serve their constituent criminal justice agencies by:

- Reducing ambiguity (by defining a statewide process for all criminal justice agencies)
- Enhancing controls and standards
- Offering consistency
- Increasing quality assurance
- Increasing compliance
- Increasing efficiency
- Providing overall cost savings

As you are aware the CJIS Security Policy has many requirements but often doesn't dictate or require a specific implementation. This is intentional and probably just as well as it provides the flexibility for each state to develop its own process fitting their needs and resources while addressing their specific state requirements. As such, each state that has implemented a centralization and coordination process for CJIS vendors has done it a little differently. States have achieved CJIS centralization and coordination at

the state level through several mechanisms: CJIS Agreements, CJIS Process Agreements, Procurement of CJIS-related Services Agreements, CJIS Vendor Management System, General Coordination Processes, etc.

It has been done - and done very successfully. How exactly it gets done is not rocket science, but it is not trivial in nature either. Assuring requirements are met and compliance is maintained is critical to helping ensure the security of our critical CJIS systems.

TASER/Axon has partnered with CJIS ACE to assist state level CSOs, ISOs and others develop, identify and implement processes in their states to streamline and centralize the above CJIS requirements to take advantage of increases in efficiency, quality assurance and overall security compliance. We've worked with many states processes and can help bring those **best practices** and our **subject matter expertise** to your state for consideration. If you'd like more information on this **free service**, contact me directly at **wtatun@cjisace.com** or **(850) 778-3207**.

William "Bill" Tatun

Bill is the Chief Information Security Officer and Director of the CJIS ACE Division at Diverse Computing (www.diversecomputing.com). He retired as a Staff Inspector with the New York State Police after a 24+ law enforcement career. Bill earned a Bachelor of Science Degree in Information Technology (Security) and holds both the CISSP and CISM security industry certifications. Throughout his career he has served on the FBI CJIS Advisory Policy Board (APB) [the group that approves recommended changes to the CJIS Security Policy to the FBI Director], on the APB CJIS Security and Access Subcommittee (Chair) [the group that originates and vets changes to the CJIS Security Policy], on the NLETS Technical Operations Committee, as the NY NLETS Representative, on the NLETS Board of Directors, as the NYS Director of Information Security and Sharing - Public Safety Cluster, as the NYS CJIS Systems Officer (CSO), as the CJIS Information Security Officer (ISO), as the NYS Police Director of Information Services, and as the Information Security Officer for both the NYS Division of Criminal Justice Services and the New York State Police.

TASER/Axon and Evidence.com

Axon creates connected technologies for truth in public safety. As a business unit of TASER International, we're building on a history of innovation in policing. Our hardware and software solutions rival the best of Silicon Valley, but they're built specifically for law enforcement. Every product from our Smart Weapons to our body-worn cameras to our digital evidence management system integrates seamlessly with one another, and often complements the systems and processes you already use.

Evidence.com is a secure, end-to-end data management system that enables new workflows for managing and sharing files. Integrating your CAD or RMS system with Evidence.com automates the process of tagging videos with complete, correct metadata. The secure Evidence.com platform lets prosecutors manage data of any type, from any agency, all in one place, while maintaining chain of custody.

Diverse Computing

Diverse Computing, Inc. is a specialty software and consulting company that develops NCIC/CJIS end-user access and message switch applications for federal, state and local criminal justice agencies. Through its CJIS Audit and Compliance Experts Division (CJIS ACE), DCI provides criminal justice agencies and vendors with a full suite of "all things CJIS" consulting services. More than 1600 agencies throughout the country utilize DCI's eAgent software and services to perform their duties every single day.