Federal, State, Tribal, and Territory ISOs,

On behalf of the FBI CJIS ISO Program staff, I am once again pleased to provide this recap of the CJIS ISO Program actions from 2015. We had a very busy and productive year and are honored to provide continual support to you, the ISO community. We are including highlights of significant events and milestones as well as a look ahead at things already on the horizon for 2016. Our continuing goal in this annual report is to present an overview of the successes achieved and the challenges faced and overcame in the previous year.

Most State ISOs have met (in person or virtually) the ISO Program Staff members. However there are several new ISOs across the community. Therefore, by way of introduction, we've included staff bios at the end of this annual update. Feel free to reach out to any member of the team or contact all of us via our iso@ic.fbi.gov email address.

LOOKING BACK AT 2015

CJIS Security Policy Publication and Maintenance

CJIS Security Policy (CSP) version 5.4 was released in October of 2015 and includes Advisory Policy Board (APB) approved changes from calendar year 2014 along with administrative updates. The new and improved "Requirements and Tiering Document" was introduced which includes the requirement tiering priorities. To recap those priorities:

- **Tier 1 requirements must be met by a system before a CSO can allow connection to the state system.**
- **Tier 2 requirements must be met by the date indicated in the plan approved by the CSO.**

APB and Compact Council Support

The ISO Program supported all APB and Compact Council meetings in 2015. The following action topic papers were prepared and presented by ISO Program staff members. Each of these topic papers went through the APB and several were also presented in the Compact Council governance process:

- Security Awareness Training Requirements – Modification of the security awareness training requirements to provide greater flexibility for individuals with only unescorted access to physically secure locations. *Results will be reflected in version 5.5*
- CJIS Systems Agency Audit of Contractor Facilities – Change allowing a CSA to conduct a compliance audits of contractor facility for another CSA. *Results will be reflected in version 5.5*
- Clarification of Out-of-Band Authentication for Advanced Authentication – Defines the meaning of out-of-band with regard to the passing of authenticators. *Results will be reflected in version 5.5*
- CJIS Systems Officer Delegation of Personnel Screening Requirements – Allows a CSO to delegate the decision for continued access to CJI by individuals with other than felonies. *Results will be reflected in version 5.5*
- Administrator Account for Least Privilege – Creates a new best practices appendix on the concept least privilege access to network information system resources. *Results will be reflected in version 5.5*
- Evaluation of Appendix K – Rewrite of the current appendix to provide greater supplemental guidance for CJIS Security Policy requirements. *Results will be reflected in version 5.5*

Outreach and Training

Outreach efforts continue be a high priority for the ISO program. Although resource constraints continue to provide challenges, the ISO program overcame and achieved a respectable level of success during 2015. The following are highlights from the year:

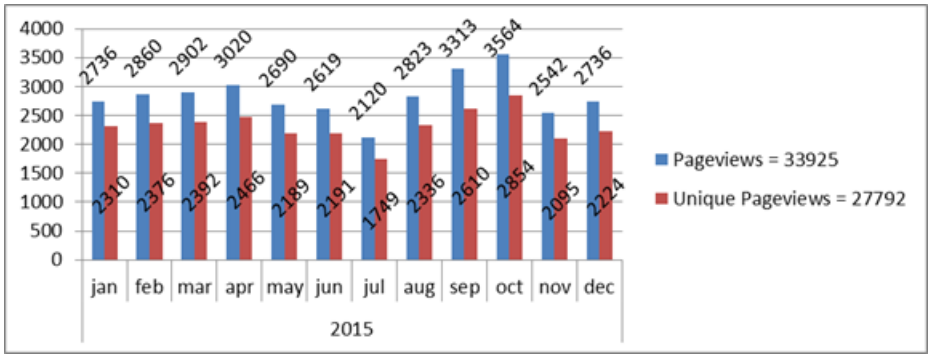
- The CJIS ISO Special Interest Group (SIG) page continues to provide information to those with access to the Law Enforcement Enterprise Portal (LEEP). The site is unrestricted and anyone with LEEP access can view the page and join the SIG. If you do not have access to this resource, we encourage you to get an identity from one of the many identity providers and take advantage of the available information.

- We are very pleased to continue our presence on the FBI.gov web site – the CJIS Security Policy Resource Center. The web site continues to provide one-stop shopping for policy resources. With the release of CSP version 5.4, there were 389 hits on the web site, the highest of any day prior. Resources currently available on the site include:
  - Current version of the CJIS Security Policy
  - Requirements and Tiering Document
  - CJIS Security Policy to NIST SP 800-53 mapping document
  - 2014 ISO Symposium Slides
  - Cloud report and control catalog
  - Mobile Appendix
  - Links of Importance page providing links to other federal government sites with security best practices and resources
  - Use Cases
  - Question submission page

The direct link to this page is:

http://www.fbi.gov/about-us/cjis/fbi-cjis-security-policy-resource-center-links-of-importance

Activity on the site is fairly consistent. As you can see below, there was a spike in October when the new version of the Policy was released, a typical trend we see each year.



Pageview — A pageview is an instance of a page being loaded by a browser. The Pageview metric is the ***total number of pages viewed***; repeated views of a single page are also counted.

Unique Pageview — A *unique pageview* represents the ***number of sessions*** during which that page was viewed one or more times.

- The ISO Program reached over 6,000 criminal justice professionals by presenting at, or supporting meetings, conferences and training events nationwide. The following is a sample of the organizations and agencies that were part of the ISO Program outreach during 2015:

  - National Conferences
    - Motorola Solutions SPSS User's Conference
    - IJIS
    - SEARCH
    - Nlets STARS Conference
    - National Association of Attorneys General
    - Center for Internet Security (webcast)
    - CJIS Tribal Conference

- State Conferences and Training
  - ILETS – Idaho
  - KCJIS – Kansas
  - SLED – South Carolina
  - GATAC – Georgia
  - CJIC – Michigan
  - CJIS – Oregon
  - CJIS – Utah
  - CJIS – Missouri
  - Florida Department of Law Enforcement (FDLE) LASO Training
  - New Jersey LASO Training Seminar
  - CJIS – Hawaii
  - New Hampshire LASO Training

TRAINING REMINDER

The Originating Agency Identifier, or ORI, is a key element in transaction validation. However, ORIs are not used by CJIS as an identity authenticator for transactions and should not be used as a mechanism for identity authentication for access to CJI. Many ORIs can be found by searching the Internet and our own policy does not protect ORIs unless associated with PII or active case, etc. Consequently, we need to guard against individuals using ORIs as a form of social engineering in a non-technical effort to gain access to CJI. To combat this type of attack, a best practice would be to not allow dissemination based solely on an individual presenting an ORI as a primary identifier. We recommend several other forms of identifying information be required prior to any dissemination.

LOOKING FORWARD TO 2016 AND ALL ITS CHALLENGES

We expect to be as busy in 2016 as the previous year with the ISO Program continuing to provide support and training for the ISO community. Many states have already contacted us with invitations to provide briefings at their conferences and we've penciled those in on the calendar. As resources allow, we will support as many requests as we can. Please let us know as far in advance as possible if you would like us to support your efforts.

From a *CJIS Security Policy* perspective, we anticipate addressing several topics through the 2016 APB. So far, these will include:

- NCIC Restricted and Non-restricted File Access and Use
- Clarifying Encryption Requirements in the *CJIS Security Policy*
- FedRAMP Vetting and the *CJIS Security Policy* Requirements
- Protecting Audio and Video Data (from body worn cameras) as Criminal Justice Information

We have finalized plans for the two and half day 2016 ISO Symposium. Mark your calendars for June 14th -16th, 2016. The venue will be the National Conference Center in Leesburg, Virginia. This outstanding conference center will provide the ISO community ample opportunities for training and networking. We will send invitations and details closer to the symposium. The tentative agenda includes time for new ISOs to meet and greet and network with the Security and Access Subcommittee members and a number of seasoned ISOs. The first half-day will focus on the essentials of being an ISO and will be open to those ISOs in their position two years or less. The full-day sessions will include keynote speakers, panels and security-centric topics intertwined and linked to the most challenging aspects of the *CJIS Security Policy*. There will be plenty of time for networking, questions, visiting the vendors and socializing and networking with ISO peers. I am excited about this opportunity for the ISO community and anticipate a great event. As always, the ISO symposium is part training, part information and part dialogue between the presenter and the audience so we encourage ISOs to come prepared with questions and an eagerness to network with fellow ISOs. I'm confident you will find great value in the symposium and interaction with the key players who affect change in the *CJIS*

Security Policy. This event will kick off an annual cycle of ISO Symposiums alternating between a full two and half day event in the even years and a one day event in odd years.

When possible, the ISO Program will continue to take advantage of opportunities to provide on-site training for agencies and organizations either in a local or regional setting. If you would like us to attend or present at your conference or event please let us know. Additionally, you are always welcome here at CJIS in "Wild and Wonderful West Virginia." We can customize training for you or any of your staff.

If you have questions, proposed solutions, need clarification on a policy situation, or want to provide feedback on the CJIS ISO Program please don't hesitate to contact us. We request you use the iso@ic.fbi.gov email address for initiating communication with us. The advantage to using this address is that your message gets to the entire team and anyone can, and will, respond to you. You may also use the FAQ submission page on the FBI.gov site. If you have LEO access, there is also a "Questions and Feedback" page on the ISO SIG site.

Thank you for all that you do,

George

George A. White
Chief, CJIS Information Assurance Unit
FBI CJIS ISO

FBI CJIS ISO Program Team BIOS

George White, CJIS ISO / Chief, CJIS Information Assurance Unit: George joined the FBI in 2006 after a 20 year career with the U.S. Air Force and two years as a contractor supporting the Joint Warfighter program. As a technical security architect, he helped jumpstart the FBI Criminal Justice Information Services (CJIS) Division's transition from an application-oriented to a services-oriented architecture. In 2008, he was assigned to manage the CJIS Information Security Officer (ISO) program and was designated the FBI CJIS Division's ISO. In addition to his ISO duties, George directs the CJIS Division's Information Assurance Unit. In this role, George oversees a team of government and contractor personnel tasked with supporting cradle to grave security of all CJIS Division services. His email address is george.white@ic.fbi.gov and his direct phone number is 304.625.5849.

John C. "Chris" Weatherly, CJIS ISO Program Manager: Chris joined the FBI in 1994 with his entire career in some flavor of security. Chris was a Federal police officer understanding the need for accurate information expeditiously. In 1998, Chris assumed the position of Personnel Security Specialist responsible for initiating and maintaining contract personnel security clearances. His current assignment, taken in 2004, Chris was assigned as an Information System Security Officer (ISSO) for several CJIS systems to include the CJISWAN, and was recently promoted to a Supervisory ISSO position overseeing ISSOs of all CJIS systems. Chris can be reached at john.weatherly@ic.fbi.gov and his direct phone number is 304.625.3660.

Jeff Campbell, CJIS Assistant ISO: Jeff came to the Bureau after a 14 year career with the U.S. Air Force followed by several years as a DoD information technology and security contractor and as a private sector information security assessor. Jeff focuses on maintaining and updating the CJIS Security Policy, crafting topic papers, supporting external conferences and seminars, and representing the program on various CJIS internal working groups (i.e. Mobility Working Group, Indian Country Working Group). His email address is jeffrey.campbell@ic.fbi.gov. His direct phone number is 304.625.4961.

Steve Exley, CJIS ISO Sr. Consultant/Technical Analyst: Steve served eight years in the U.S. Army as part of the Signal Corps working on both tactical and strategic communications maintenance and security for both U.S. and NATO commands. Prior to joining the CJIS ISO Program team in February of 2011, he worked as contractor for seven years at Ft. Belvoir, VA serving as an Information Assurance Security Officer (IASO), a Ports, Protocols, and Services

Manager (PPSM), and a Computer Network Defense (CND) Information Analyst for the US Army Cyber (ARCYBER) Command. Steve is the point person on several continuous efforts including: white papers and best practice guidance development, Use Case and FAQ development, CSP Resource Center web site content maintenance, technical desktop analysis for network and product solution implementations submitted by the CJIS community, and APB topic papers. His email is stephen.exley@ic.fbi.gov and his direct phone number is 304.625.2670.

Jeff Campbell, CISSP
Assistant Information Security Officer
FBI/CJIS Division/CIAU/ISO Program Office
1000 Custer Hollow Rd.
Clarksburg, WV 26306
304.625.4961 (office) | 304.476.4711 (mobile)
304.625.3638 (fax)