



Names of key clients, key client organizations

Ohio Office of Criminal Justice Services

- David Lewis
- Jerry Zachariah

Names of IJIS Institute consultants and their firms

Walter Coleman, ACS Inc.

Greg Duncan, PEC Solutions

Dates services were provided

May 2 – June 3, 2003

Overview of client need, high-level statement of work

The OCJS requested the IJIS Institute provide security consultants under its Technology Assistance project to:

- Review existing materials on the OJIN project and recommend a security solution utilizing the most current and effective technology.
 - Identify security issues and compliance per the Criminal Justice Information System (CJIS) Security Policy Document, focusing on the Technical Security section of the document and touching on other sections where appropriate¹.
 - Define steps, approaches, and technologies to resolve these security issues. Recommendations should include high-level architecture or technology options, as well as a high-level summary of the types of hardware and software solutions that support the proposed options.
- Review the drafted Memorandum of Understanding (MOU) to be used for both the contributors and users who wish to participate and/or use OJIN.
 - Validate that the MOU addresses the security requirements third parties must abide by before participating in the OJIN.
 - Identify needed changes to the MOU, if any, so that the MOU complies with technical security requirements mandated in the Federal CJIS Policy Document.
- Provide OCJS officials with a short report documenting
 - Recommendations for general OJIN technical architecture designs and technologies to resolve identified OJIN security issues and comply with the CJIS Security Policy Document. Each recommendation should include:
 - The range of hardware and software solutions that support the architecture design or recommended technology; and
 - A high-level description outlining the complexity of architecture or technology installation and needed levels of staff training.
 - Any updates and/or suggestions to the reviewed MOU so that it complies with security requirements mandated in the Federal CJIS Policy Document.

¹ The CJIS document is set forth by the Federal Bureau of Investigation (FBI). OCJS officials must consider these recommendations before moving to full implementation of OJIN.

Type of Service Provided (teleconference, on-site visits and reports)

On May 7 and 8, 2003 the IJIS Institute consultants conducted a site-visit to the OCJS offices in Columbus, OH. During the site visit, the consultants conducted a series of meetings and interviews. Upon arriving at the OCJS offices on May 7, the consultants met with and interviewed David Lewis and Jerry Zachariah in an effort to organize their initial findings of the OJIN project. Their initial findings were based on their review of OJIN documentation provided by the OCJS and an initial conference call conducted between the IJIS Institute consultants, Mr. Lewis, and Mr. Zachariah on May 2, 2003. During the afternoon of May 7, the IJIS Institute consultants began developing their formal recommendations for the OCJS and reconvened with Mr. Lewis and Mr. Zachariah in the evening to discuss their preliminary recommendations and further clarify aspects of the OJIN project. On May 8 the IJIS Institute consultants continued to develop their recommendations for the OCJS until they briefed Mr. Lewis and Mr. Zachariah in the afternoon with their final recommendations. The final report was delivered to OCJS on June 3, 2003.

Outcomes/Considerations

Based on the IJIS Institute's findings, the consultants recommend a multi-phased deployment of the internet-based OJIN system that will accomplish the OCJS goals for OJIN and achieve *Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Security Policy* compliance. Phase I includes the use of Secure Sockets Layer (SSL) sessions which provides an acceptable degree of data confidentiality through encryption without an undue technical, fiscal and management burden. The more complex Phase II introduces the use of Virtual Private Network (VPN) technologies and continues using the SSL infrastructure established in Phase I. The result will be a system that supports mobile users and utilizes two layers of encryption, through a VPN using the Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) and SSL sessions using public-key encryption by way of digital certificates.