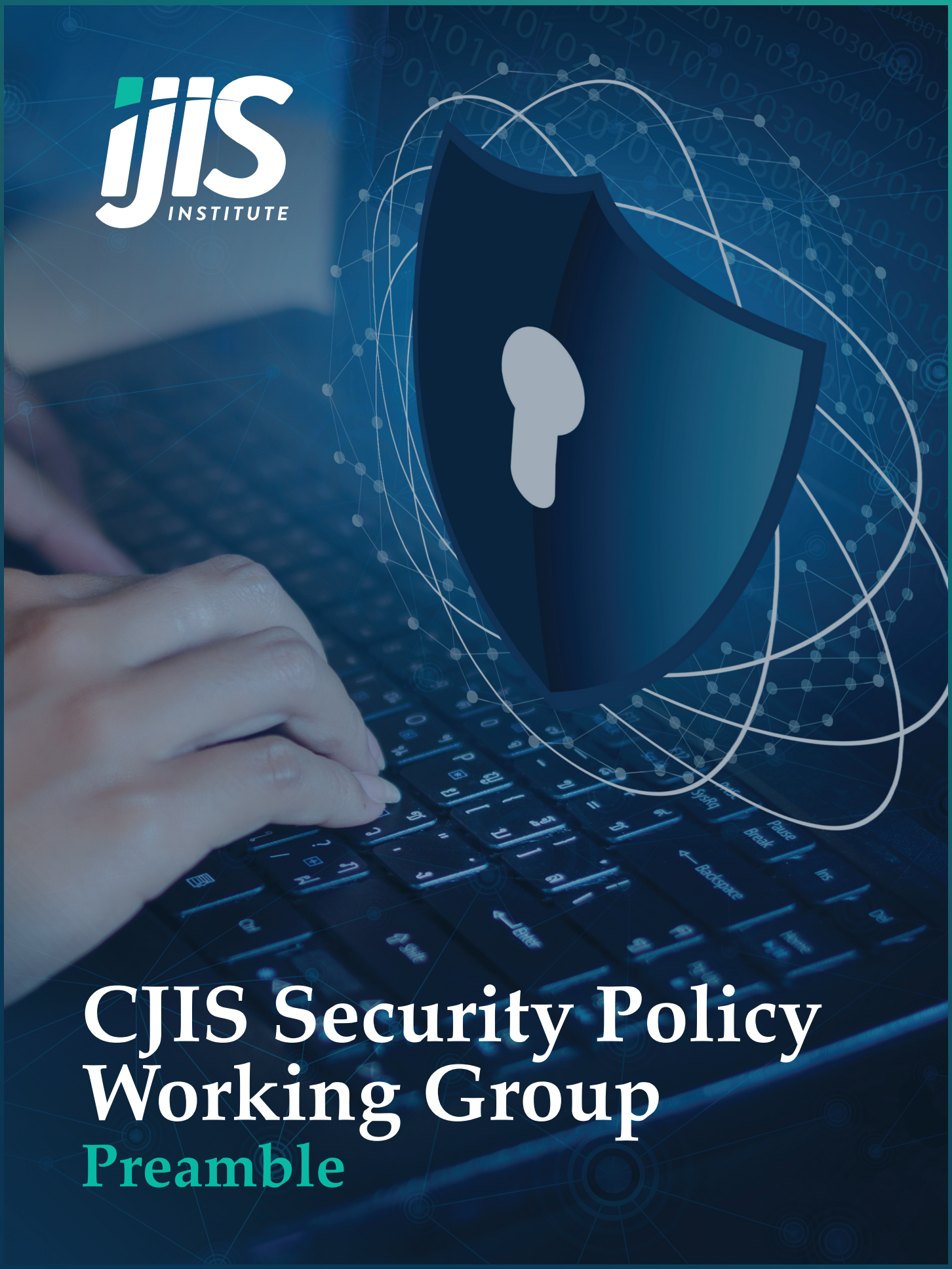

CJIS Security Policy Working Group

Preamble

Acknowledgements

This document is a product of the IJIS Institute; a nonprofit collaboration network that brings together innovative thinkers from the public and private sectors, national practice associations, and academic / research organizations working together to solve public sector mission, information sharing, policy and technology challenges.

IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

IJIS CJIS Security Policy Work Group Roster

Charlie Schaeffer, Chair	*Microsoft/Azure*
Jens Black	*Motorola Solutions*
Gerard Britton	*Enforsys Inc.*
Jeff Campbell	*FBI CJIS*
Ed Claughton	*PRI Management Group*
Monty Coats	*South Carolina Law Enforcement Division (SLED)*
Holden Cross	*FBI CJIS*
Brian DaSilva	*Mark43*
Matthew Doherty	*Sikich*
Jim Emerson	*NW3C*
Jason Emineth	*equivant*
Gerard Gallant	*Amazon Web Services*
Mike Lesko	*NEC*
Catherine Miller	*Montgomery County Maryland Police*
Maury Mitchell	*Alabama Law Enforcement Agency*
JC North	*Nlets*
Greg Park	*Livermore Police Department, CA*
Bill Philips	*Nlets*
Rob Serio	*Computer Projects of Illinois*
John Tomme	*Analysts*
George Vit	*South Brunswick, NJ Police Department*
Catherine Watson	*AT&T*
Chris Weatherly	*FBI CJIS*

Comments and Questions? They are always welcome! Please contact the IJIS Institute at **info@ijis.org** or **703-726-3697**.

Introduction

The CJIS Security Policy serves as a critical resource for criminal justice agencies by offering guidelines and best practices to protect the integrity, confidentiality, and availability of Criminal Justice Information (CJI). It provides rigorous security requirements, policies, and controls that must be implemented to maintain the trust and reliability of those maintaining and accessing this information. The CJIS Security Policy incorporates executive orders, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) recommendations, and nationally recognized guidance from the National Institute of Standards and Technology.

As technology and innovation continue to advance at an unprecedented pace, ensuring the security of sensitive information is paramount for entities storing and requesting access to CJI. With these critical needs in mind, the Federal Bureau of Investigation (FBI) continues to update the Criminal Justice Information Services (CJIS) Security Policy to provide a comprehensive framework for safeguarding data in an ever-changing environment.

Given the complex and constantly evolving policy requirements, it is imperative to have avenues to simplify and educate the stakeholder community, which includes but is not limited to criminal justice and law enforcement agencies, private sector service providers, nonprofit and academia organizations supporting the public sector community. The IJIS Institute remains committed to filling that obligation by partnering with FBI CJIS and key representatives from the stakeholder community.

IJIS Institute CJIS Security Policy Working Group

In December of 2022, through collaboration with the FBI CJIS Division, the IJIS Institute created a CJIS Security Policy Working Group. After assessing the needs of the stakeholder community, the Working Group objectives include but are not limited to assessing the impacts of the CJIS security policy's alignment with the broader security controls (i.e., NIST 800-53), and coordinating educational and informational campaigns and instructional series. The creation of this group enables IJIS to inform our community of the impact on current operational processes, technology impacts, and implementation guidelines.

What's Next?

To support its charter, this Working Group has collaborated directly with representatives from FBI CJIS to offer several educational webinars and in-person workshops to review the policy changes in versions 5.9.1 and 5.9.2. Over the next several weeks and months, the Institute will be releasing a variety of companion documents to educate State and Local criminal justice agencies further, as well as the Service Providers offering solutions in this space on the operational, technical, and fiscal impacts of the approved changes in v. 5.9.2. The Working Group will be publishing companion documents for the following control families, which were identified as the most pressing and underpublicized changes for additional clarification:

- **Section 5.2: Awareness and Training**
- **Section 5.6: Identification and Authentication**
- **Section 5.8: Media Protection**
- **Section 5.14: Unsupported System Components**

These releases will help the public sector user community and support service providers with abbreviated and consumable resources to understand the policy's impacts on their systems and processes. While this publication series will concentrate specifically on the updates from v. 5.9.2, the working group will remain committed to providing educational opportunities through webinars, companion documents, etc., on the approved and published versions of the CJIS Security Policy. These resources aim to review the policy changes and educate the stakeholder community on the impacts and value of CJIS Security Policy compliance.