



CISA
CYBER+INFRASTRUCTURE



Interagency Security Committee

2019 Annual Report

MARCH 2020



The Survivor Tree at the Oklahoma National Memorial and Museum - this American elm tree, located a few yards away from the Oklahoma City, OK bombing site, withstood the destruction of one of the worst terrorist attacks on American soil on April 19, 1995.

Photo Credit: Oklahoma City National Memorial & Museum

Message from the Chair



Logo Credit: Oklahoma City
National Memorial & Museum

I am pleased to present the Interagency Security Committee (ISC) 2019 Annual Report. As we look back on the significant accomplishments of 2019, we need to pause and acknowledge the importance of the upcoming year which will mark both the 25th Anniversary of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, OK and in its wake, the creation of the ISC. The Anniversary theme of “Looking Back, Thinking Forward” is particularly appropriate in this regard.

This report highlights many of the accomplishments and activities of the ISC in 2019 – in particular, the updating and publishing of several important guidance documents, another successful year of taking the Risk Management Process and Facility Security Committee training to our stakeholders across the country, and notably completing our first year of compliance reporting. The completion of this year’s inaugural round of compliance reporting is a major milestone towards meeting the final remaining requirement from Executive Order (EO) 12977.

The report also showcases the great work the ISC expects to conduct in the coming year. While much has been accomplished over these last 25 years, more remains to be done. Please see the section on The Way Forward to learn about the continued progress we have planned for 2020, as well as our plans to support the 25th Anniversary of the Oklahoma City Bombing in April and observe the ISC’s 25th Anniversary in October.

Finally, I want to thank the members of the ISC who volunteer their time, share their expertise and provide leadership to the efforts of the ISC. This annual report is a testament to their steadfast efforts and their commitment to defend today and secure tomorrow. I thank them for their continued dedication to the important mission of securing and protecting federal facilities.

Brian Harrell

Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency

Table of Contents

	Executive Summary	1		Training	5
	Compliance	2		Outreach	8
	Policies, Standards & Recommendations	4		The Way Forward	11

Executive Summary



Credit: Oklahoma City National Memorial & Museum

The ISC was established by EO 12977 six months after the worst incident of domestic terrorism in the history of the United States. In about a month, we will mark the 25th Anniversary of this event that killed 168 individuals, including 19 children at the onsite childcare facility at 9:02 A.M. on April 19, 1995.

The mission of the ISC is to enhance the quality and effectiveness of security in, and protection of, facilities in the United States occupied by federal employees for nonmilitary activities. The ISC is a permanent interagency body that addresses continuing government-wide security concerns.

This Annual Report provides stakeholders with a snapshot of the Committee's activities and accomplishments over the course of 2019 and highlights plans and initiatives for 2020. Please take a moment to review the significant accomplishments and performance of the ISC this past year and to rededicate our collective efforts to continuing that progress in 2020. This report is organized by major ISC lines of effort: Compliance; Policies, Standards and Recommendations; Training; and Outreach.

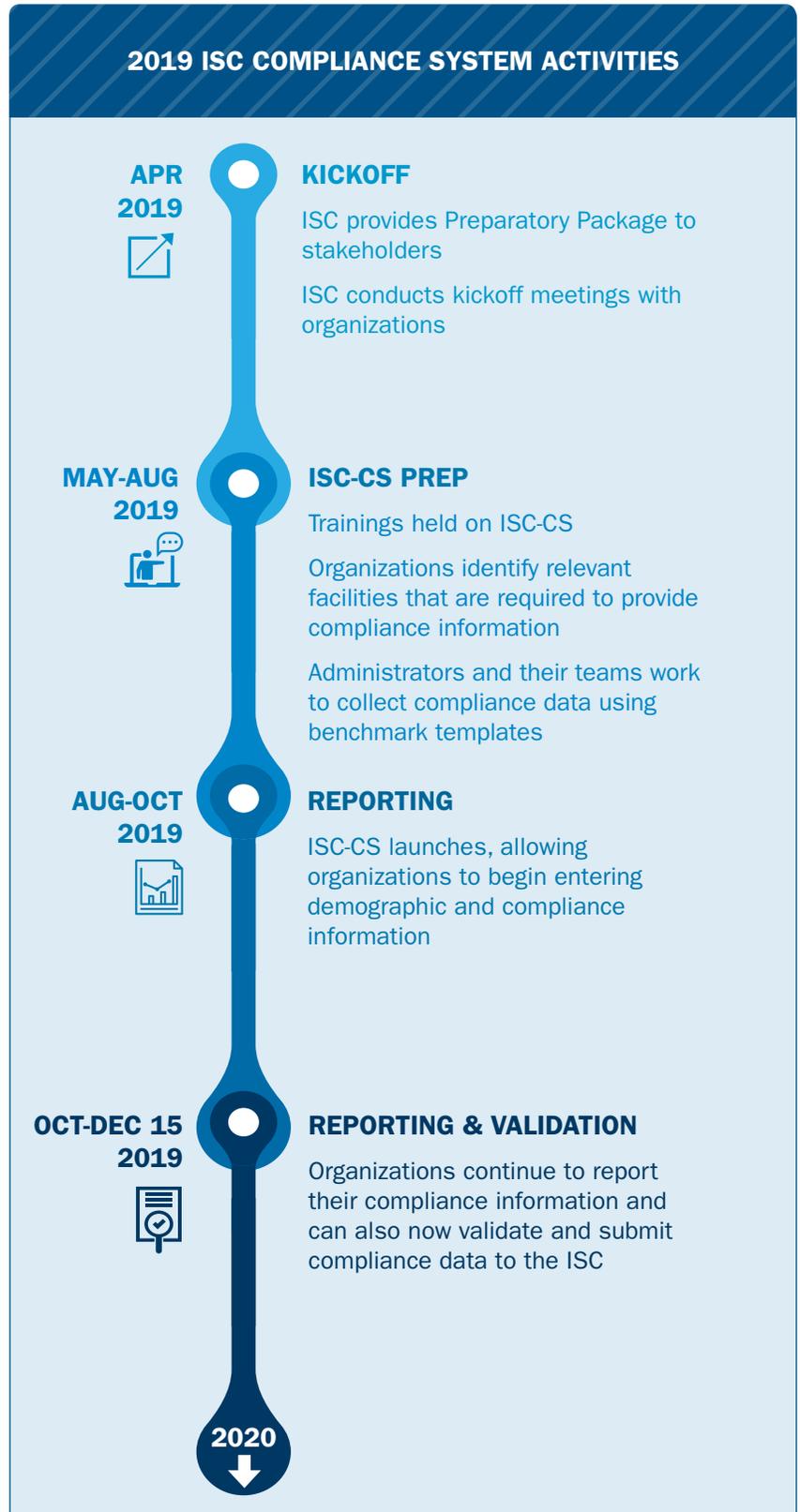
Compliance



EO 12977 requires the ISC to “develop a strategy for ensuring compliance” with ISC policies and standards. In 2019, the ISC fully deployed the ISC Compliance System (ISC-CS) and completed its inaugural year of compliance reporting, a major milestone towards meeting the final remaining requirement from EO 12977.



The result of this first year of compliance reporting was an overwhelming success, with a response rate of 71.4 percent. In total, 81 percent of ISC’s Primary Members¹ and 67 percent of Associate Members² participated in the fiscal year 2019 Compliance Reporting. Thanks to the dedication of participating members, the ISC has gained greater insight into the level of compliance nationwide and will use analysis of this data to focus resources in a number of areas – from engagement and training efforts to refining policies and standards to targeted assistance.



1. Primary Members are the 21 federal departments and agencies designated by EO 12977 and modified by EO 13286.
 2. Associate members petition to join the ISC and are approved by the Steering Subcommittee and the ISC Chair.



TOTAL NUMBERS REPORTED



Organizational Benchmarks Submitted
159



Facility Benchmarks Submitted
5,255

AGENCY ASSISTANCE

The ISC provided over
250
instances of agency assistance from
August – December 2019.

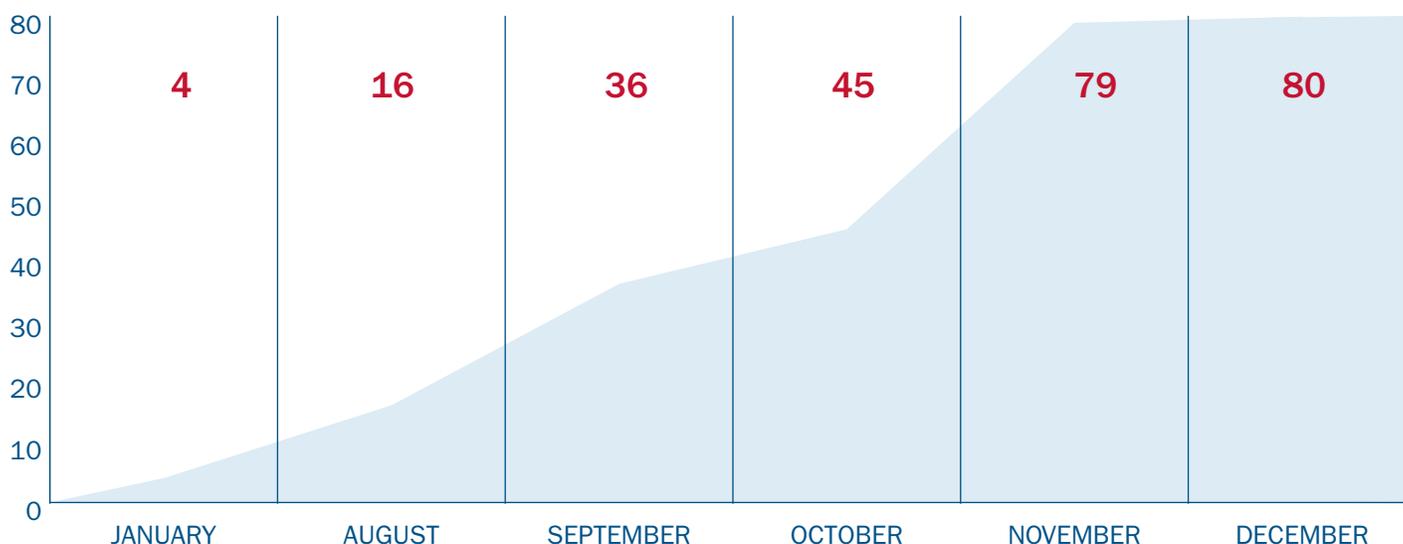
OTHER METRICS

Of the **45** organizations that reported compliance information, another **118** of their sub-organizations or components entered compliance information.

3 non-executive branch agencies found value in compliance reporting, as did **1** of our newest members with less than a year with the ISC.

Compliance Assistance

Assisting ISC-CS users with the new system and understanding the benchmarks was a major component of the ISC's inaugural year of reporting. In 2019, ISC staff conducted over 250 instances of assistance to ISC-CS users from more than 65 organizations. This had a direct, positive effect in the high response rate that we received.





Policies, Standards & Recommendations

ISC policies, standards and recommendations serve as a collaborative roadmap to keep people safe and secure in federal facilities. In 2019, the ISC updated 6 guidance documents including substantive updates to both the *Violence in the Federal Workplace: A Guide for Prevention and Response* and *Armed Contract Security Officers in Federal Facilities: An Interagency Security Committee Best Practice*.

VIOLENCE IN THE FEDERAL WORKPLACE KEY UPDATES



- Includes a section on the Behavioral Risk Assessment Process
- Emphasizes synchronizing efforts with the organization's Insider Threat Program
- Includes considerations for revocation of access after termination
- Provides additional emphasis on other forms of workplace violence to include bullying
- Expands guidance on utilizing physical security measures
- Reorganizes Appendix A (Threat Assessment, Countermeasures, Awareness, Resources, and Case Studies) into three separate appendices on Awareness, Resources and Case Studies

Link to publication: <https://www.cisa.gov/publication/isc-violence-federal-workplace-guide>

ARMED CONTRACT SECURITY OFFICERS IN FEDERAL FACILITIES KEY UPDATES



- Defines the functions of a contract security force as a threat countermeasure
- Lists the minimum criteria for suitability, physical, medical, training/education, experience, grooming/appearance, uniforms, and equipment
- Provides factors that estimate security staffing levels for specific security posts

Link to publication: <https://www.cisa.gov/sites/default/files/publications/digital-strategy/Armed%20Contract%20Security%20Officers%20in%20Federal%20Facilities-An%20ISC%20Best%20Practice%202019.pdf>

OTHER UPDATES

The ISC also published updates to three of the appendices to *The Risk Management Process (RMP) for Federal Facilities: An Interagency Security Committee Standard*:

[Appendix A: The Design-Basis Threat Report 2019 edition key updates](#)

The Baseline Threat Rating increased for two Undesirable Events (UE) and decreased for three other UEs based on an analysis of recent events and the planning and organizational skills required

[Appendix B: Countermeasures and Appendix C: Child Care Centers Level of Protection Template 2019 edition key updates](#)

A comprehensive update was made on the requirements of an Occupant Emergency Plan as required by Title 41 of the Code of Federal Regulations

Additionally, revised to reflect updates to the recently published Design-Basis Threat Report

REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide was also updated

Training

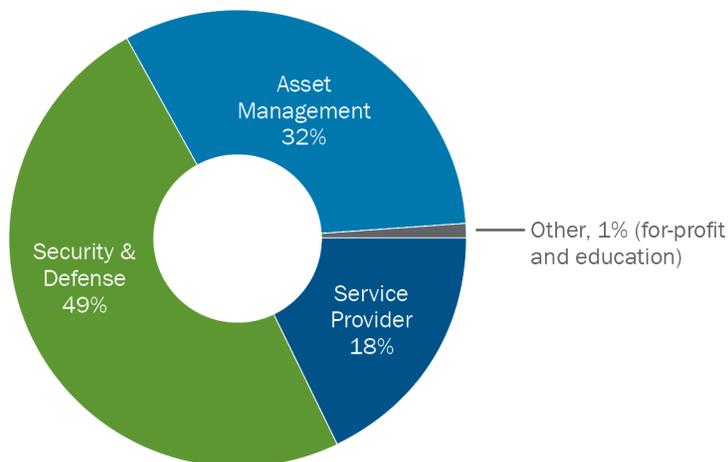


To better educate stakeholders on ISC Policies and Standards, the ISC developed the Risk Management Process and Facility Security Committee (RMP FSC) training as a component of its National Compliance Advisory Initiative (NCAI). This half day, instructor-led training course, which serves as a prerequisite for Facility Security Committee (FSC) membership, covers the ISC RMP and the roles and responsibilities of FSC members. The target audience includes FSC Chairs, FSC Members, Executives, Managers, and any personnel involved in making facility funding, leasing, security, or other risk management decisions.



In 2019 the RMP FSC, through partnership with the Cybersecurity and Infrastructure Security Agency's Office for Bombing Prevention Accreditation authority, became the first and only ISC RMP to provide Continuing Education Units (CEUs) through the International Association for Continuing Education and Training (IACET). Accreditation through IACET is a major milestone in the history of ISC training and professional recognition for its quality.

RMP FSC 2019 Metrics



921 | Participants

93% | Average Exam Score

99% | Positive Composite Feedback Score

74 | Participating Departments, Agencies and Organizations

Individual Participant Numbers

Primary	579
Associate	279
Non-Member	63
State	26
Local	8
Other (includes Universities, Non-Profit Organizations, etc.)	20
Private (includes representatives from Amazon and Starbucks)	9

166 (18%) of trainees represent departments, agencies, or organizations whose mission it is to provide a service to the U.S. public.

Department of Veterans Affairs (VA), Social Security Administration (SSA), and U.S. Department of Agriculture (USDA)*

292 (32%) of trainees represent departments, agencies, or organizations that manage and oversee resources.

General Services Administration (GSA), Office of Personnel Management (OPM), and Internal Revenue Service (IRS)*

453 (49%) of trainees represent departments, agencies, or organizations that secure or defend U.S. infrastructure, information, or people.

Federal Protective Service (FPS), Department of Homeland Security (DHS HQ), and Department of Defense (DOD)*

*Agencies listed above represent a sampling of participating agencies.



Federal Risk Management Process Training Program (Fed RMPTP) Certifies its 1,000th Student

For the past 8 years, the Office of Personnel Management (OPM) has hosted numerous 3-Day Fed RMPTP courses which teach students how to develop a Facility Security Level (FSL), identify various levels of protection and gain a deeper understanding of the ISC's RMP.

In September of 2019, a course was held in Oklahoma City, OK, where students were able to visit the Oklahoma City National Memorial and Museum at the site of the Alfred P. Murrah Federal Building bombing. During this course, OPM certified its 1,000th student, marking a significant accomplishment in the program's history. The ISC would like to congratulate the Fed RMPTP students, as well as the instructors, for reaching this significant milestone.

AMERICAN SECURITY TODAY 'ASTORS' HOMELAND SECURITY AWARDS



In November, the **Fed RMPTP** received four awards from **American Security Today 'ASTORS' Homeland Security Awards** for:



**BEST CRITICAL
INFRASTRUCTURE
PROTECTION
PROGRAM**



**BEST LAW
ENFORCEMENT
COUNTER TERRORISM,
CRIME PREVENTION
PROGRAM FOR FED/
STATE/LOCAL**

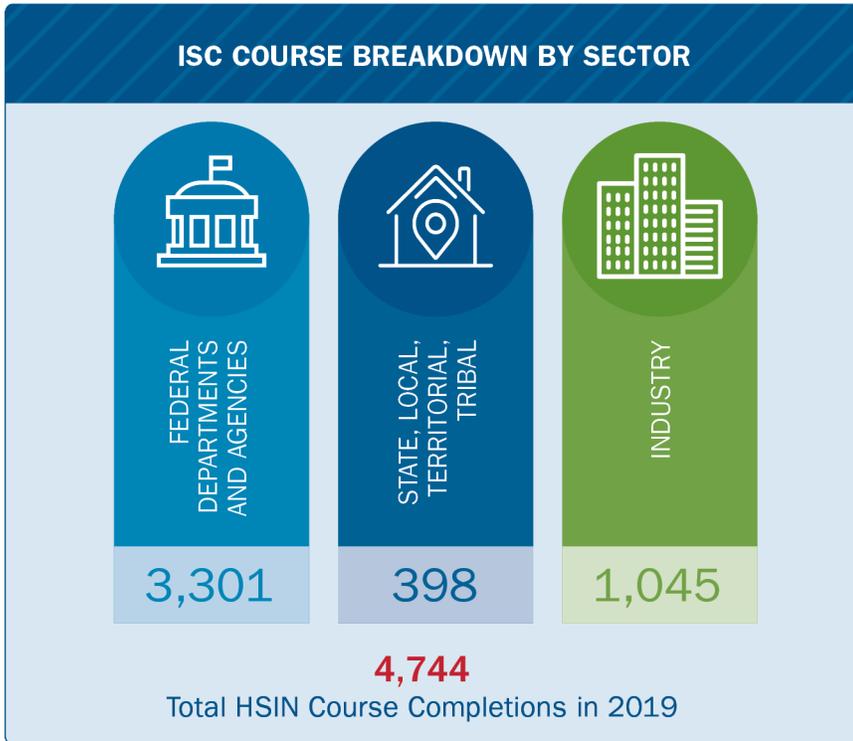


**BEST FEDERAL
GOVERNMENT
SECURITY PROGRAM**



**EXCELLENCE IN
PUBLIC SAFETY**

These noteworthy accomplishments speak to the quality of the program and the acknowledgement of its importance by the federal security community.



Online Homeland Security Information Network Trainings

The Homeland Security Information Network (HSIN) provides users with online versions of the ISC’s RMP FSC training modules. The ISC developed these online training courses to educate stakeholders on ISC security policies, standards, and recommendations. The training course is comprised of five lessons: Introduction to the ISC; Overview of ISC Publications; RMP for Federal Facilities: FSL Determination; Levels of Protection (LOP) and Application of the Design-Basis Threat Report (For Official Use Only); and FSC.

Webinars

To support its training objectives, the ISC occasionally hosts webinars to better educate stakeholders on a variety of security-related topics. In 2019, the ISC held a webinar entitled, *Violence in the Federal Workplace: A Guide for Prevention and Response*. The webinar drew attendance from 222 federal and non-federal stakeholders and aligns with the ISC’s guide of the same title updated in 2019.



Outreach



New Members

Along with 21 ISC Primary Members who were included in EO 12977, the ISC is also made up of numerous Associate Members. In 2019, the ISC inducted three new Associate Members: the International Boundary Water Commission (IBWC), the Railroad Retirement Board (RRB), and the Federal Energy Regulatory Commission (FERC). As of December 2019, the ISC has 63 Primary and Associate Members in total.



ISC IN THE NEWS



Critical Infrastructure Security and Resilience – Today and Tomorrow
– Security Magazine

<https://www.securitymagazine.com/articles/91018-critical-infrastructure-security-and-resilience-today-and-tomorrow>



Anti-bullying Policies Should be Leading Indicators
– EHS Today

<https://www.ehstoday.com/ehs-outloud-blog/article/21120100/antibullying-policies-should-be-leading-indicators>

COMPLIANCE ASSISTANCE HIGHLIGHT – ISC ASSISTS STAKEHOLDER WITH FACILITY ACCESS ISSUES

Part of the ISC’s remit to “enhance the quality and effectiveness of security” across the federal landscape includes as-needed, hands-on assistance to stakeholders. Compliance assistance encompasses a variety of activities, including help with compliance reporting, guidance on policies and standards, strategic communications, and tools and trainings support.

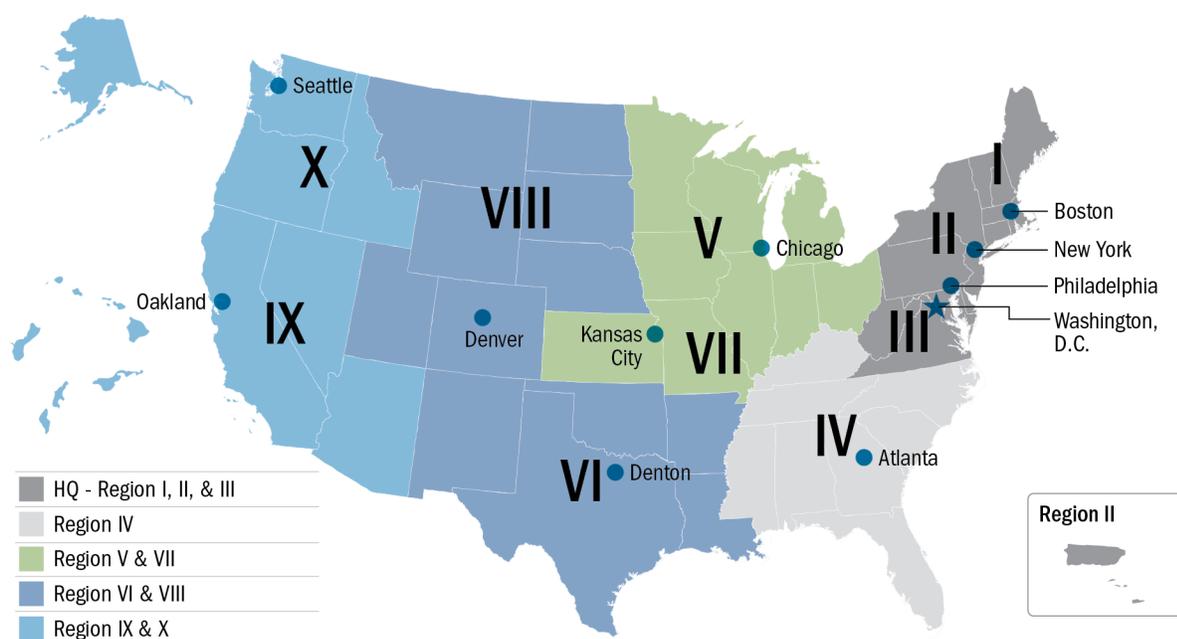
In the Spring of 2019, ISC staff were contacted to provide support for a stakeholder located in the National Capital Region in a multi-tenant, government-owned facility. Due to several contractual stipulations, the leasing authority and the tenants of the facility manage different access control and screening points. As a result, each access control point conducted security screening in a different way, leading to confusion and misalignment among facility stakeholders.

The tenants, leasing authority, security organization, and FSC were unable to come to a consensus on how to address their facility’s current screening policy. As a result, the ISC was brought in to assist. After assessing the security situation, ISC staff provided their expert opinion on the matter, as well as several recommendations for a path forward. The ISC encouraged the stakeholders to review their current risk assessment, document all remedial actions, including their consultation with the ISC, and present their findings to the FSC. After acting upon these recommendations, the facility stakeholders joined the ISC’s Facility Access Control Working Group, so they could share their experience and gain useful insights from other members on matters related to access control.



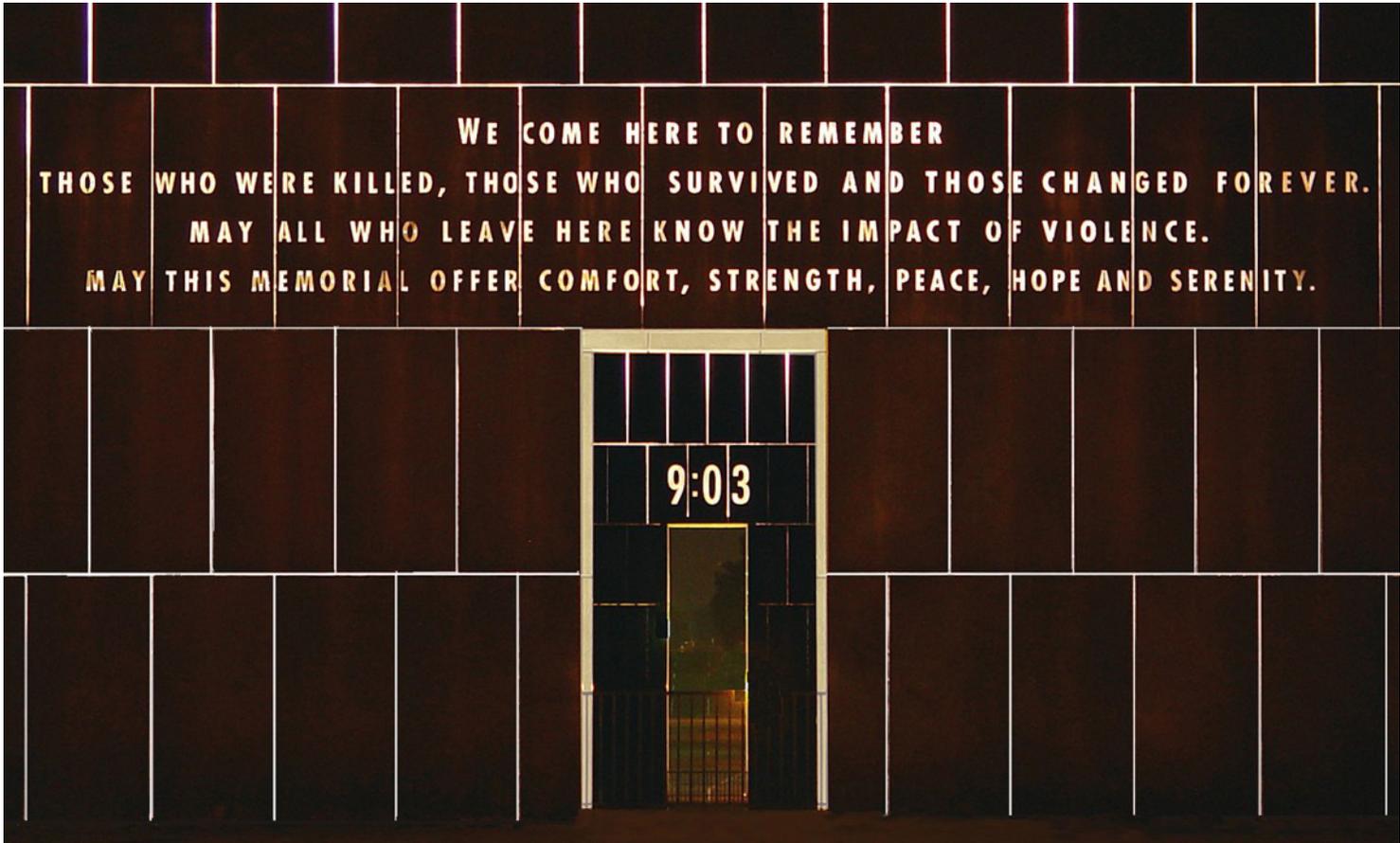
Regional Advisor Updates

The ISC's Regional Advisors provide a significant and visible commitment to federal facility stakeholders outside of the National Capital Region. In 2019, ISC Regional Advisors continued to expand their outreach efforts and capacity building with regional stakeholders. Regional staff helped to train more than 800 regional stakeholders and liaised with numerous agency representatives. To better understand the scope of the positive impact of their work, a few select highlights are listed below.



*Cities listed on map represent regional office locations

REGIONS I - III	Provided one-on-one support to an FSC chair on how to increase tenant engagement and increase productivity of FSC meetings.
REGION IV	Provided an explanation of the ISC-CS and an overview of FSC roles and responsibilities to the Internal Revenue Service and General Services Administration (GSA) leadership, security specialists and business managers at their Fall Symposium.
REGIONS V, VII	Assisted RRB in becoming an ISC Associate Member.
REGIONS VI, VIII	Hosted the first ever FSC discussion webinar which provided an opportunity for federal multi-tenant stakeholders to share FSC best practices and lessons learned. The success of the webinar sparked the development of a new FSC.
REGIONS IX, X	Collaborated with the GSA Office of Mission Assurance in Region X to draft a guide for standing up an FSC and provided compliance overviews to Federal Executive Boards (FEB) Directors, GSA Regional Administrators and FPS Regional Directors.



Credit: Oklahoma City National Memorial & Museum

The Way Forward



COMPLIANCE

The ISC will refine the ISC-CS and the reporting process as a result of lessons learned during 2019.

In 2020, ISC members will have a full year to access the system and input their compliance information.



POLICIES, STANDARDS & RECOMMENDATIONS

The ISC will complete and publish *Best Practices for Protecting Against the Threat of Unmanned Aircraft Systems (UAS): An Interagency Security Committee Guide*. This new guidance will address UAS risk assessments, protection activities, increasing workforce awareness, engaging with community partners, developing a response plan and emergency action plans.

In 2020, the ISC will complete and publish *Facility Access Control Best Practices: An Interagency Security Committee Guide*. The Guide examines stakeholder entry eligibility, screening processes and escort procedures to name a few.

The RMP Standard will be reviewed and updated, as needed, and a new working group to update the active shooter policy will be established.

The Convergence Subcommittee will begin work on building a guidance document focused on achieving unity of effort between the physical, operational technology and informational technology domains.



TRAINING

The ISC is developing the next phase of its NCAI: A Facility Security Committee Workshop. This effort is aimed at helping FSCs develop and refine those products, processes and procedures necessary to meet their responsibilities.



OUTREACH

The ISC will continue its commemorative communications surrounding the 25th Anniversary of the Oklahoma City, OK bombing and the 25th Anniversary of the creation of the ISC.

The ISC will support the 25th Anniversary Remembrance Ceremony on April 19, 2020 in Oklahoma City, OK.

The ISC will observe its 25th Anniversary on October 19, 2020 in Washington D.C.



Front Cover Credit: Thurgood Marshall Federal Judiciary Building, Washington, D.C.
Back Cover Credit: Oklahoma City National Memorial & Museum

For general inquiries, including questions for
ISC Staff and Regional Advisors, please contact
[**ISC@hq.dhs.gov**](mailto:ISC@hq.dhs.gov)

For access to ISC Publications, please contact
[**ISCAccess@hq.dhs.gov**](mailto:ISCAccess@hq.dhs.gov)

For questions related to the rollout of the
Compliance System, please contact
[**ISCCS-Support@hq.dhs.gov**](mailto:ISCCS-Support@hq.dhs.gov)



CISA
CYBER+INFRASTRUCTURE

