Law Enforcement Cyber Center

Final Technical Report

Sasha Romanosky, Karlyn D. Stanley, Jirka Taylor, Zev Winkelman

Prepared for the Bureau of Justice Assistance
Preface

The Bureau of Justice Assistance established a Law Enforcement Cyber Center (LECC) in October 2014 to help local and state law enforcement better combat cybercrime. The LECC, which completed activities in September 2017, was managed by a consortium of organizations and led by the RAND Corporation as the main grantee. The LECC’s partner organizations were the International Association of Chiefs of Police and the Police Executive Research Forum. This report summarizes the activities of the LECC, which aimed to raise the awareness and enhance the education and capacity of criminal justice and public safety agencies with respect to cyber threats and cybercrimes. This report is primarily intended for the Bureau of Justice Assistance but may also be of interest to others working in the field of cybercrime.

This project was supported by Grant No. 2014-D6-BX-K012 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice’s Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The research reported here was conducted in the RAND Justice Policy Program, which spans both criminal and civil justice system issues with such topics as public safety, effective policing, police–community relations, drug policy and enforcement, corrections policy, use of technology in law enforcement, tort reform, catastrophe and mass-injury compensation, court resourcing, and insurance regulation. Program research is supported by government agencies, foundations, and the private sector.

RAND Justice, Infrastructure, and Environment (JIE) conducts research and analysis in civil and criminal justice, infrastructure development and financing, environmental policy, transportation planning and technology, immigration and border protection, public and occupational safety, energy policy, science and innovation policy, space, telecommunications, and trends and implications of artificial intelligence and other computational technologies.

Questions or comments about this report should be sent to the project leader, Karlyn Stanley (kstanley@rand.org). For more information about RAND Justice Policy, see www.rand.org/jie/justice-policy or contact the director at justice@rand.org.
Contents

Preface ............................................................................................................................................ iii
Box, Figures, and Tables ................................................................................................................ v
Summary ........................................................................................................................................ vi
Acknowledgments .......................................................................................................................... ix
Abbreviations .................................................................................................................................. x
1. Overview..................................................................................................................................... 1
2. The LECC Team Designed and Built a Dedicated Website ....................................................... 3
   Development of the LECC Website .............................................................................................. 3
   Continuous Efforts to Improve User Experience ........................................................................ 3
   LECC Web-Traffic Statistics ........................................................................................................ 7
3. LECC-Provided Access to a Range of Training Resources ...................................................... 10
   Development of Training Materials ............................................................................................ 10
   Efforts to Identify External Contributors .................................................................................. 11
4. LECC’s List of Regional Capabilities Helped Link Crime Units ............................................. 15
   Development of Regional Capabilities List ................................................................................ 15
5. LECC Developed Prevention-Focused Resources .................................................................... 17
6. LECC Report on the Utah Model Offered Technical Assistance ............................................. 20
7. Justice Executive Cyber Roundtable Brought Together Key Stakeholder Groups 
   to Discuss Cyber-Related Issues ............................................................................................... 22
8. LECC Complied with All Administrative Requirements ......................................................... 24
   Reporting Arrangements ............................................................................................................. 24
   Transition to NW3C ..................................................................................................................... 24
9. Conclusions and Recommendations ......................................................................................... 25

Appendixes
A. List of Delivered Training and Technical Assистances ............................................................ 27
B. List of LECC Deliverables ....................................................................................................... 29
C. List of Justice Executive Cyber Roundtable Attendees ........................................................... 30
D. Justice Executive Cyber Roundtable Agenda .......................................................................... 33
E. LECC Promotional Brochure ................................................................................................... 35

References ..................................................................................................................................... 37
Box, Figures, and Tables

Box

Box 7.1. Key Concerns and Challenges Identified at the
Justice Executive Cyber Roundtable ........................................................................................................ 23

Figures

Figure S.1. Trends in Semiannual Traffic to LECC Website
(Aggregated Reporting Periods for Sessions and Page Views).................................................................... vii
Figure 2.1. Trends in Monthly Traffic to the LECC Website (First Months of
Reporting Periods for Sessions and Page Views) ......................................................................................... 7
Figure 2.2. Trends in Semiannual Traffic to the LECC Website
(Aggregated Reporting Periods for Sessions and Page Views) ......................................................................... 8
Figure 3.1. LECC “Training” Page ............................................................................................................... 10
Figure 3.2. LECC “Chiefs’ Corner” Page ....................................................................................................... 13
Figure 4.1. Search Interface of the Directory of Cybercrime Labs and Resources ........................................... 16
Figure 5.1. “Cybercrime Community Awareness and Prevention” Section
of the LECC Website ..................................................................................................................................... 18
Figure E.1. LECC Promotional Brochure, Page 1 ............................................................................................ 35
Figure E.2. LECC Promotional Brochure, Page 2 ............................................................................................ 36

Tables

Table S.1. Overview of LECC Tasks and Corresponding Activities and Indicators.................... vi
Table 1.2. Overview of LECC Tasks and Corresponding Activities and Indicators ......................... 2
Table 2.1. Geographical Dispersion of LECC Website Visitors .......................................................... 9
Table A.1. List of LECC Training and Technical Assistance .............................................................. 27
Table B.1. List of LECC Deliverables ........................................................................................................... 29
Summary

Cybercrime and cyber threats place many demands on law enforcement agencies, ranging from investigating cyber incidents to securing their own information systems. In addition, law enforcement agencies are required to collect and handle the constantly increasing volume of digital evidence. The Bureau of Justice Assistance (BJA) established the Law Enforcement Cyber Center (LECC) in October 2014 to help state and local law enforcement better combat cybercrime. The LECC, which completed activities in September 2017, was tasked to serve as an online portal and a clearinghouse of information, directing users to existing resources developed and managed by subject-matter experts, professional organizations, and government agencies.

The LECC was managed by a consortium of organizations led by the RAND Corporation as the main grantee. Partner organizations on the LECC team were the International Association of Chiefs of Police (IACP) and the Police Executive Research Forum (PERF). Although not formally part of the LECC grant, the project team also collaborated with the National White Collar Crime Center (NW3C), a nonprofit organization. This report provides an account of LECC activities since its inception in October 2014 to its completion in September 2017.

The report is organized by the LECC’s main tasks and activities, as summarized in Table S.1.

Table S.1. Overview of LECC Tasks and Corresponding Activities and Indicators

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Corresponding Activities and Indicators</th>
</tr>
</thead>
</table>
| 1. Design and build cyber center              | 1a. Development of the LECC website  
|                                               | 1b. Continuous efforts to improve user experience  
|                                               | 1c. Continuous efforts to promote the LECC and its website  
|                                               | 1d. Web-traffic statistics                                                                          |
| 2. Identify cybercrime training and training gaps | 2a. Development of training materials for groups (e.g., chiefs, officers, investigators and prosecutors) targeted by the website |
|                                               | 2b. Efforts to identify relevant content and external contributors                                  |
| 3. Link crime units                           | 3a. Development of regional capabilities list                                                          |
| 5. Technical assistance                       | 5a. Report on development of a cybercrime center                                                      |
| 6. Justice Executive Cyber Roundtable         | Not applicable                                                                                       |
| 7. Administrative requirements                | 7a. Reporting arrangements                                                                            |
|                                               | 7b. Transition to NW3C                                                                                |

Design and Build Cyber Center

The project team developed and launched a dedicated LECC website and undertook continuous efforts to improve the experience of its users. These efforts encompassed making
changes to the website based on external feedback, as well as based on an analysis of traffic patterns on the website. Concurrently, the project team undertook efforts to promote the website at various meetings, fora, and conferences, making use of a promotional brochure developed for this purpose. Web-traffic statistics show that over the course of its operation, the LECC website enjoyed significant growth in the volume of users, as measured by the number of web sessions and page views. Looking at the last three full reporting periods, the number of sessions increased 130 percent when comparing the first half of 2016 and 2017, and the number of page views went up 114 percent over the same period of time (see Figure S.1).

Figure S.1. Trends in Semiannual Traffic to LECC Website (Aggregated Reporting Periods for Sessions and Page Views)

Identify Cybercrime Training and Training Gaps

To provide content related to training on the LECC website, the project team developed dedicated sections with links to existing resources and enabled users to access relevant information. The team also established methods to identify potential new content for the website, helping to ensure that information available on the LECC website remained up-to-date, relevant, and of interest to its users. In addition, the project team collaborated with external contributors who provided content for various sections of the website.

Link Crime Units

The objective of the list was to help LECC website visitors identify and contact organizations, experts, and practitioners who could assist cyber-related investigations and prosecutions. To that end, the LECC team compiled a list of U.S. regional capabilities relevant for combating cybercrime, such as forensics labs or training facilities. The list was converted to a
searchable database to enhance its utility for users. The database grew to contain 1,007 entries, representing, to our knowledge, the most comprehensive resource available for this type of information.

Prevention Education

To enhance cybercrime prevention, the LECC website hosted a series of educational materials and tools intended to help raise users’ awareness and assist their cybercrime prevention efforts. One of the most notable items in this category was “Pokémon Go: A Law Enforcement Alert” and an accompanying video. The video explained the Pokémon Go application and its potential effect for law enforcement. The video was one of the most popular items on the LECC website, generating more than 2,000 views. As with training materials, the LECC team put in place processes to identify new relevant material and potential external contributors. In addition, the project team also coordinated its prevention activities with external ongoing efforts—for instance, by coordinating web postings and linking to information provided by other initiatives such as the National Cybersecurity Awareness Month.

Technical Assistance

In a major technical assistance effort, the LECC team developed a report on the implementation of the Utah Model of cybercrime prevention, summarizing lessons and best practices from the implementation of a new cybercrime unit in Utah. The report built on a series of interviews with groups of stakeholders in Utah, as well as with representatives of other cybercrime units. It was designed as a resource for other agencies that are in the process of or are contemplating establishing a cybercrime unit.

Justice Executive Cyber Roundtable

In March 2017, the LECC team convened a Justice Executive Cyber Roundtable, bringing together representatives of various stakeholder groups, including police chiefs, investigators, prosecutors, and judges. The roundtable consisted of a series of panel discussions and facilitated working groups aiming to foster dialogue and exchange of information and experience across the various groups of participants. The discussions also resulted in the identification of the most serious cybercrime-related challenges and best practices in the fight against cybercrime.

Administrative Requirements

Simultaneously with all the aforementioned activities, the LECC team adhered to all agreed reporting requirements.
Acknowledgments

This report was made possible through a grant from the Bureau of Justice Assistance at the U.S. Department of Justice. We are grateful to our project officers, James Patrick McCreary and David Lewis, for their assistance throughout the project.

This project was a partnership between the RAND Corporation, the International Association of Chiefs of Police, and the Police Executive Research Forum. We are grateful to all of the staff who participated in the development and implementation of this project. We would also like to thank our peer reviewers, Meagan Cahill at the RAND Corporation and Patrick Mays at the Office of the State’s Attorney for Montgomery County, Maryland.
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>BJA</td>
<td>Bureau of Justice Assistance</td>
</tr>
<tr>
<td>CCDE</td>
<td>Computer Crime and Digital Evidence</td>
</tr>
<tr>
<td>CJTFG</td>
<td>Criminal Justice Technology Forecasting Group</td>
</tr>
<tr>
<td>DHS</td>
<td>U.S. Department of Homeland Security</td>
</tr>
<tr>
<td>DOJ</td>
<td>U.S. Department of Justice</td>
</tr>
<tr>
<td>DPS</td>
<td>Utah Department of Public Safety</td>
</tr>
<tr>
<td>ESI</td>
<td>electronically stored information</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>IACP</td>
<td>International Association of Chiefs of Police</td>
</tr>
<tr>
<td>LECC</td>
<td>Law Enforcement Cyber Center</td>
</tr>
<tr>
<td>LEIM</td>
<td>Law Enforcement Information Management</td>
</tr>
<tr>
<td>NW3C</td>
<td>National White Collar Crime Center</td>
</tr>
<tr>
<td>PERF</td>
<td>Police Executive Research Forum</td>
</tr>
<tr>
<td>RSS</td>
<td>Rich Site Summary</td>
</tr>
<tr>
<td>TTA</td>
<td>training and technical assistance</td>
</tr>
</tbody>
</table>
1. Overview

Cybercrime is a serious threat that poses substantial risks to national security, economic welfare, and public safety. It puts pressure on law enforcement agencies tasked with investigating various forms of cybercrimes and cyber threats coming from criminals and state actors alike. In addition to investigative responsibilities, law enforcement agencies also need to protect their own information systems from being compromised by cyber criminals. Furthermore, criminal justice agencies need to cope with increasing volumes of electronic evidence, as virtually all criminal incidents are likely to involve digital evidence in some form. This places a requirement on law enforcement officials to be proficient in collecting, handling, and securing this type of evidence and its many novel forms.

In response to these challenges, the Bureau of Justice Assistance (BJA) established the Law Enforcement Cyber Center (LECC) to help state and local law enforcement better combat cybercrime. The LECC was tasked to serve as an online portal and a clearinghouse of information, directing users to existing resources developed and managed by subject-matter experts, professional organizations, and government agencies. In doing so, the LECC aimed to raise the awareness and enhance the education and capacity of criminal justice and public safety agencies with respect to cyber threats and cybercrimes. This included the ability to prevent as well as respond, investigate, and prosecute these types of incidents.

The LECC was managed by a consortium of organizations led by the RAND Corporation as the main grantee. Partner organizations in the LECC team were the International Association of Chiefs of Police (IACP) and the Police Executive Research Forum (PERF). Although not formally part of the LECC grant, the project team also collaborated with the National White Collar Crime Center (NW3C), a congressionally funded nonprofit organization.

This report provides an account of LECC activities since its inception in October 2014 to its completion in September 2017. Main activities of the LECC project team, however, concluded in April 2017 when the management of the LECC transitioned to the NW3C under a different funding arrangement. Therefore, the last six months of the original grant duration were focused on ensuring a smooth transition of LECC ownership and end-of-grant reporting and other administrative requirements.

This report is organized by the LECC’s main tasks. Initially, seven tasks were proposed for the center:

- survey
- design and build cyber center
- identify training and training gaps
- link crime units
- prevention education
• administrative requirements
• pilots and technical assistance.

After a kick-off meeting with the BJA, these tasks were changed, and the survey and pilots were taken out of the project tasks. Instead, a technical assistance document geared toward the development of a cybercrime center was added. In addition, in March 2017, the LECC organized the Justice Executive Cyber Roundtable. The event represented the culmination of LECC activities in 2017 and linked all of the LECC tasks outlined.

Table 1.2 summarizes the project’s final set of tasks and corresponding activities and indicators, which are discussed in greater detail in the remainder of this report. Because of its cross-cutting character and its size, the Justice Executive Cyber Roundtable is covered in a separate section.

Table 1.2. Overview of LECC Tasks and Corresponding Activities and Indicators

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Corresponding Activities and Indicators</th>
</tr>
</thead>
</table>
| 1. Design and build cyber center  | 1a. Development of the LECC website  
1b. Continuous efforts to improve user experience  
1c. Continuous efforts to promote the LECC and its website  
1d. Web-traffic statistics         |
| 2. Identify cybercrime training   | 2a. Development of training materials for groups (e.g., chiefs, officers, investigators and prosecutors) targeted by the website  
2b. Efforts to identify relevant content and external contributors |
| and training gaps                 |                                                                                                          |
| 3. Link crime units               | 3a. Development of Regional Capabilities List                                                                  |
7. Administrative requirements    | Not applicable  
7a. Reporting arrangements  
7b. Transition to NW3C |
|                                  |                                                                                                          |
2. The LECC Team Designed and Built a Dedicated Website

Development of the LECC Website

The development of the LECC website started immediately following the project’s kick-off meeting. The framework design and the scope of the LECC website underwent a series of reviews by the task team and the wider project team, with each revised version incorporating received comments. A similar process was adopted for the site’s content, which was developed based on team discussions and reviews.

In the process of developing the website, the project team encountered and overcame two technical issues. The project team decided to contract with a web-hosting company to implement a new website framework. Outsourcing the technical aspects of the website development accelerated the creation of the website, as well as its subsequent updates. Second, the project team encountered issues with the process for modifying the website’s content across partnering agencies. The project team worked successfully with Matrix, the website development contractor, to streamline the process for editing content.

Following the completion of the preparatory work, a demonstration site was developed and piloted with partner agencies. These agencies reviewed the site and its content; this feedback was further incorporated into the site’s design. A soft launch of the website occurred on April 17, 2015, and the public launch took place at the Law Enforcement Information Management (LEIM) conference sponsored by the International Association of Chiefs of Police on May 18, 2015.

Continuous Efforts to Improve User Experience

Following the launch of the LECC website, the project team engaged in continuous efforts to improve user experience on the site. Activities in this area fell broadly into three groups: (1) soliciting feedback from users, (2) working to understand the site’s traffic patterns, and (3) making informed amendments to the website. We discuss all three types of efforts in the next sections.

Feedback from Users

The project team undertook a series of steps to gather feedback about and suggestions to improve the site and generate more users. One step was the development and deployment of a user assessment, sent to individuals on partner listservs and contacts generated through the development of the LECC website. Individual recipients were asked to provide information on themselves, their agencies, their interests, and to provide feedback on the site and suggestions for future materials or topics. The project team received 198 responses, mostly from local law
enforcement agencies. Respondents filled various roles in these agencies (e.g., chiefs and officers), with a relatively uniform distribution of interests (e.g., crime investigations, digital evidence, prosecution). Respondents also represented local and state fusion and intelligence centers. The results of the assessment indicated that most respondents were not aware of the LECC; approximately 80 percent had not visited the site before receiving the invitation to participate. Upon review, most responded that they were satisfied with the LECC design and content, with positive responses to the training, news/blogs, and resource center. No responses included comments for improvements or for additional content areas.

Another mechanism to capture feedback from users was the introduction in the first half of 2016 of a new feature to the website asking users about the utility of a given item. The feature was located after each article and content page and took the form of the question “Was this article helpful?” The response options were initially limited to “yes” and “no,” with accompanying thumbs up or down. Subsequently, those who indicated that information was not helpful were also invited to provide additional information, although this step was optional and did not yield substantial actionable feedback. According to an analysis conducted at the end of the relevant reporting period, 75 percent of responses were “yes” and 25 percent “no.” The articles rated as the most helpful were “Rather than Fearing ‘Cyber 9/11,’ Prepare for ‘Cyber Katrina,’” and the internet of things infographic.

In another effort to solicit feedback from actual and potential users, project staff reached out directly to a local law enforcement agency. The team met with police officers from Anne Arundel County in Maryland, with whom members of the project team had developed working relationships and who agreed to review and discuss the website with LECC staff. The officers provided feedback on various aspects of the LECC, as well as insights on what they look for in an information resource. To illustrate, officers

- stressed the desirability of having a “one-stop shop” for information and of the ability to find information within two clicks
- volunteered that they mostly seek local resources and/or information applicable locally
- expressed preference for additional infographic-type information and for fewer text-heavy pages
- suggested that there be more emphasis to the training links, including providing a direct link to the training section to the top navigation bar
- appreciated the possibility to use the search bar.

Similarly, the project team reached out to various prosecutors’ offices to solicit feedback from the perspective of this type of user. The project team interviewed prosecutors in numerous offices, including the following: Bell County, Texas, District Attorney’s Office; Mississippi Attorney General’s Office; Orange County, California, District Attorney’s Office; Wayne County, Michigan, District Attorney’s Office; U.S. Attorney’s Office, Washington, D.C.; and Massachusetts Attorney General’s Office, Boston, Massachusetts.
Understanding Traffic Patterns

Complementing information obtained directly from actual and potential users, the project team also gathered data on web traffic on the LECC website. These data were collected through the development of an automated analytical report, selecting Google Analytics as the analytical platform.

Data obtained through Google Analytics provided information on a series of variables, including the number of users, their location, what pages they visit, how long they stay on the website and on a page, and whether they return (results are presented later in this chapter).

In addition, in late 2016, members of the research team undertook a review of the LECC website and its information flows. The review also made use of information available from Google Analytics regarding what content tends to be viewed by which types of users and how they access it. The objective of this activity was to ensure that, given the constantly growing content on the LECC website, information is easily and promptly accessible and the site remains user-friendly in its navigability. This activity subsequently fed into discussions about a possible redesign of the website’s landing page (see the next section).

Amending the LECC Website

The project team used the information gleaned from the activities listed in the previous section to continuously amend the LECC website to improve the site’s utility and the experience of its users. These activities were undertaken in parallel with efforts to develop new content for the website, which are described in Chapters Three and Five of this report.

Examples of steps taken to make the site more user-friendly include the following:

- **Site navigation:** A checklist was developed to help provide users with an overview of and assistance navigating the website.
- **Prosecutor’s page:** The content devoted to prosecutors was redesigned.
- **Training page:** The training page was redesigned to allow users to differentiate among the types of training offered by different agencies.
- **Redesign of homepage:** The project team implemented a better homepage for the website that provided an introduction to assist users with the website layout.
- **Logo:** The LECC project team developed a new logo for the website, which is now on the website and all project materials.
- **Search engine for regional capabilities:** Another issue was the best way to provide the regional capabilities list (see Chapter Four) in a way that would be most helpful to

---

1 While the identity of visitors to the website remained unknown, for the purposes of mapping traffic patterns, the project team developed a typology of users based on the categories of stakeholders targeted by the LECC website—chiefs, officers, prosecutors, and investigators. A visitor was assigned to a user category if his or her first page was either the landing page or the main page for a given stakeholder group and his or her second to fourth viewed page were also part of the same stakeholder group link on the LECC page. This categorization is for obvious reasons based on a series of assumptions and may be subject to inaccuracies; however, the project team agreed it represents a reasonable approximation and a useful insight into users’ behavior while on the LECC website.
agencies. The original list, which was hundreds of pages long, was converted to a searchable database, called the “Directory of Cybercrime Labs and Resources.”

In addition, building on the information from Google Analytics and learning from NW3C’s experience with the redevelopment of its website, the project team developed in January 2017 a series of mock-ups for a comprehensive redesign of the LECC website landing page. The objective of this effort was to make the landing page more user-friendly and help users better navigate the LECC website and the resources available there. Building on internal discussions and input from BJA, the project team worked with Matrix (an external web developer) to build a development site for the new LECC landing page. The purpose of the new development site was to demonstrate how the new layout would look and work in practice on all types of devices (i.e., including mobile devices). A decision of how to proceed with the redesign had not been taken by the end of the project.

Continuous Efforts to Promote the LECC and Its Website

To promote the LECC website, the project team created a one-page brochure that provided an overview of the LECC and its content (see Appendix E for an example). The purpose of the brochure, in addition to being made available on the LECC website, was to have it serve as a quick reference resource to present at meetings and conferences and to distribute to relevant target audiences. To that end, the project team identified a series of conferences to determine which ones would be appropriate to request distribution of the LECC brochure in conference materials. Examples of conferences where members of the project team distributed the brochure and other promotional materials include:

- IACP and LEIM Training Conference and Technology Exposition (May 2016)
- Criminal Justice Technology Forecasting Group (CJTFG) meeting (January 2016)
- Summer Quarterly Meeting of the Washington Metro Electronic Crimes Task Force (August 2016)
- Cyber Situational Awareness and Information Sharing conference at George Mason University (September 2016)
- IACP annual conference in San Diego (October 2016).

Additional meetings and conferences where members of the project team promoted the LECC are listed in Appendix A.

In other promotional activities, LECC partner agencies were requested to include the brochure in their training materials and, if appropriate, to provide a link to the LECC website from their own websites. Agencies that agreed to do so included the NW3C, the Federal Law Enforcement Training Centers, and the National Consortium for Justice Information and Statistics (SEARCH), with a combined potential reach of more than 65,000 law enforcement officers.
In addition, project staff prepared in 2016 an article for submission to *Police Beat* magazine to introduce the LECC to officers who were not yet familiar with the website. The article outlined the purpose and utility of the LECC website and invited new users to provide feedback. The LECC project team also made use of an opportunity to highlight a section of the LECC website in a half-page ad about the LECC in *Police Chief* magazine.

**LECC Web-Traffic Statistics**

Since its introduction, the LECC website has seen a continuous growth in traffic. Figure 2.1 shows the growth in monthly sessions and page views by domestic users (i.e., traffic coming from the United States\(^2\)) at the beginning of the last three semiannual reporting periods.\(^3\) It shows that between January 2016 and January 2017, the number of sessions grew 192 percent, and the number of page views grew 163 percent.

**Figure 2.1. Trends in Monthly Traffic to the LECC Website (First Months of Reporting Periods for Sessions and Page Views)**

A similar trend can be observed when the data for all three reporting periods are aggregated (see Figure 2.2). Measured this way, the number of sessions increased 130 percent when comparing the first half of 2016 and 2017, and the number of page views went up 114 percent over the same period.

\(^2\) This analysis focuses on domestic users because they represent the primary target audience of the LECC. The number of foreign users was smaller than that of domestic users.

\(^3\) The first full semiannual reporting period following the introduction of the LECC website is omitted because the team adopted Google Analytics only in fall 2015.
In contrast with traffic volume data, long-term trends in the average duration of a session or the number of pages viewed per session stayed relatively constant during all the reporting periods. Data collected through Google Analytics show that the average length of a web session by visitors to the LECC website ranged between 90 and 120 seconds,\textsuperscript{4} with values recorded only occasionally outside this range (e.g., 122 seconds in March 2016 and 85 seconds in January 2017, to illustrate deviations on both ends of the range). Another illustration of the lack of a discernible trend in session lengths is the fact that the value recorded in January 2016 (103 seconds) is very similar to that recorded in June 2017 (108 seconds).

Similarly, the number of pages visitors viewed in each session remained relatively stable, at slightly fewer than two pages per session. The highest value (1.99) was recorded in May 2016 and the lowest value (1.68) was recorded in December 2016. However, there were notable differences in the number of sessions depending on what content visitors viewed. For instance, traffic to the news and blogs section had a much higher number (typically in excess of four) of pages viewed per session, suggesting the content provided in those sections was successful in keeping visitors engaged.

Data available through Google Analytics also helped the project team understand where visitors to the LECC website come from. Perhaps unsurprisingly, the majority of visitors came from a relatively small number of large metropolitan areas. These are summarized in Table 3.1, including a breakdown by user type based on an analysis of traffic patterns of users conducted in October 2016.

\textsuperscript{4} We do not have any industry benchmarks for typical or aspirational lengths of web sessions for websites targeting law enforcement.
Table 2.1. Geographical Dispersion of LECC Website Visitors

<table>
<thead>
<tr>
<th>Category of Users</th>
<th>Most Frequent Places of Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>All users</td>
<td>Washington, D.C.; New York; Los Angeles; Chicago; Atlanta; Houston; Dallas; Arlington, Virginia; and Phoenix, Arizona</td>
</tr>
<tr>
<td>News readers</td>
<td>Washington, D.C.; Arlington, Virginia; Alexandria, Virginia; New York; Los Angeles and Santa Monica; Houston; Austin; Chicago; Bay Area, California</td>
</tr>
<tr>
<td>Chiefs</td>
<td>Washington, D.C.; Colorado Springs; Arlington, Virginia; Phoenix, Arizona; New York; Los Angeles and Santa Monica; Boston; Dallas; Chicago; Philadelphia</td>
</tr>
<tr>
<td>Officers</td>
<td>Washington, D.C.; Los Angeles and Santa Monica; New York; Arlington, Virginia; Houston; Phoenix, Arizona; Chicago; Dallas; Austin; Boston</td>
</tr>
<tr>
<td>Prosecutors</td>
<td>Washington, D.C.; New York; Los Angeles and Santa Monica; Arlington, Virginia; Alexandria, Virginia; Chicago; Boston; Bay Area, California; Atlanta; Raleigh, North Carolina</td>
</tr>
<tr>
<td>Investigators</td>
<td>New York; Washington, D.C.; Los Angeles and Santa Monica; Chicago; Houston; Dallas; Atlanta; Philadelphia; San Antonio, Texas</td>
</tr>
</tbody>
</table>

NOTE: Underlying data are from an analysis of traffic patterns conducted in October 2016.

The analysis of specific types of users also revealed the following:

- Almost one-half (49 percent) of **news readers** begin their sessions directly from the news page. This suggests that they had the link bookmarked or saved, but it could also mean that they clicked on a link shared with them. Roughly one-third of news readers (35 percent) start on the homepage and then move to the news section.
- Of those who start on a **chiefs** page, 65 percent continue to a second chiefs page. Of these visitors, 67 percent continue onto a third page, and 82 percent of those onto a fourth page.
- Of those who start on an **officers** page, 74 percent continue to a second officers page. Of these, 70 percent continue onto a third page, and 80 percent of those onto a fourth page.
- Of those who start on a **prosecutors** page, 82 percent continue to a second prosecutor page. Four-fifths (81 percent) of these users continue onto a third page and, of those, 84 percent proceed onto a fourth page.
- Of those who start on an **investigators** page, 78 percent continue to a second investigator page. Of these visitors, 70 percent continue to a third page and 77 percent of those onto a fourth page.

With respect to traffic-related individual content pages, training resources were consistently the most frequently visited section of the website, followed by, depending on the month in question, content on cybercrime investigations (under the “investigators” tab) or information on digital evidence (under the “officers” tab). The development of training materials, the most frequently visited resources on the LECC website, was the objective of the task discussed in the next chapter.
3. LECC-Provided Access to a Range of Training Resources

Development of Training Materials

Training materials made available on the LECC website are organized by the four stakeholder groups targeted by the website (i.e., chiefs, officers, investigators, and prosecutors) and, as discussed in Chapter Two, have consistently represented the most-visited section of the LECC website. The “Training” section provided an overview of agencies offering training with links to training pages and calendars. Throughout the project, LECC staff updated this section on a continuous basis to make sure the information provided remained current and relevant.

Figure 3.1. LECC “Training” Page

<table>
<thead>
<tr>
<th>IT Security</th>
<th>Cyber Crime Investigations</th>
<th>Digital Evidence</th>
<th>Legal Considerations</th>
<th>Training</th>
<th>Cyber and IT Certifications</th>
<th>Free Training for Law Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Many state, nonprofit, and private organizations have been increasing their cyber training programs in order to cope with the increased risk of cyber threats, and resulting demand for trained cyber professionals. Below we provide a list of some of these training resources available.

For information about IT and cyber certifications, please see the Cyber and IT Certifications page, and for information about training opportunities specific to individual positions and tasks, visit the National Initiative for Cybersecurity Careers and Studies (NICCS), part of the DHS and NIST National Initiative for Cybersecurity Education (NICE).

**Defense Cyber Crime Center (DC3)**

DC3's mission is to deliver superior digital forensics and multimedia lab services, cyber technical training, research, development, testing and evaluation, and cyber analysis capabilities supporting cyber counterintelligence and counterterrorism, criminal investigations, intrusion forensics, law enforcement, intelligence community, critical infrastructure partners, and information operations for the Department of Defense. DC3 offers the Defense Cyber Investigations Training Academy (DCITA), providing classroom and web-based cyber investigative and incident response training to Department of Defense agencies to protect information systems from unauthorized use, and criminal, fraudulent, and foreign intelligence activities.

<table>
<thead>
<tr>
<th>Free courses available?</th>
<th>In-person?</th>
<th>Online?</th>
<th>Sophistication (novice-expert)</th>
<th>Topics covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free, but must be federal agency, or under MOU</td>
<td>Yes</td>
<td>Yes</td>
<td>All levels</td>
<td>Computer search and seizure, Network Intrusions, Digital forensics, Basic and advanced forensic examination, Online undercover techniques</td>
</tr>
</tbody>
</table>
In addition to links to relevant training provided by various agencies, the LECC website also contained resources that visitors to the website could use. For instance, the project team developed a section on reporting cyber incidents (see Law Enforcement Cyber Center, undated[d]). The page provided resources both for law enforcement agencies that are victims of cybercrime and also for private companies and citizens reporting incidents to law enforcement. Similarly, the project team also developed a section of the website dedicated to prosecutors. Examples of the section’s content include general legal resources, relevant case law and federal statutes, litigation guides, sources for emerging legal and policy issues, and links to training. Project staff also obtained examples of actual search warrants from state attorneys general’s offices, which were then redacted so that they could be used as a generic template. These templates, as well as an accompanying guidance for use of the search warrants, were reviewed by attorneys in the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice (DOJ). The templates and guidance were made available on the prosecutor’s page.

Several additional features of the LECC website offered information for users that might be helpful in identifying and addressing their training needs. The *Cyber Beat Blog* was a regularly updated repository of summaries of various cyber-related topics that typically included links to more resources or contact information where readers could follow up for further information. Topics covered by the *Cyber Beat Blog* ranged from protection from cyber threats to criminal justice information sharing.

News stories posted on the landing page of the LECC website were also potential sources of relevant information. To identify content for this section, in 2016, the project team began working with two RSS (Rich Site Summary) aggregators—Google and Primal—to select items that may be of interest to the cybercrime law enforcement community. A project member reviewed identified news stories daily, made a selection of the most appropriate and relevant items, and uploaded them to the LECC website. Once the RSS-based search for news items was fully established, cyber-related news stories were uploaded to the website almost daily.

In addition to being a source of information, the news page may have also functioned as a mechanism for the recruitment and retention of visitors. Flow analysis of website traffic patterns of news readers conducted by members of the project team showed that almost half of readers began their session directly on the news page.

**Efforts to Identify External Contributors**

In addition to identifying relevant content by members of the project team, LECC staff also worked to identify external contributors who would be interested and willing to provide content for the LECC website. Frequently, these efforts took the form of reaching out to potential contributors at events, meetings, and conferences. To illustrate, four members of the LECC project team attended and participated in the IACP annual conference in October 2016. Our
IACP project members distributed LECC brochures at every cyber-related panel discussion at the IACP conference, and two project members attended the Computer Crime and Digital Evidence (CCDE) committee meeting on October 15, 2016. The CCDE committee meeting discussed outreach efforts for the LECC and obtained volunteers to assist with both outreach and new content for the LECC website. Similarly, in January 2017, a project member attended the Washington Metropolitan Electronic Crimes Task Force, hosted by the U.S. Department of Homeland Security (DHS) and U.S. Secret Service, and met with representatives from DHS and the Federal Bureau of Investigation (FBI) working on cybercrime. Two speakers spoke at the meeting and covered issues relevant to the LECC website. The LECC team reached out to the speakers to discuss the possibility of their contributing to the website’s content.

As a result of this outreach, external contributors authored a series of items posted on the LECC website. For instance, police chiefs contacted by the LECC team provided material for the site’s “Chiefs’ Corner.” Since the inception of the LECC website, 28 entries were posted on the “Chiefs’ Corner.”
Partner agencies were also a source of relevant material. For instance, in February 2017, the LECC website began hosting cyber alerts developed by NW3C. The cyber alerts, featured on the website’s landing page, provided information on novel online platforms and applications and their features and functions. The objective of the cyber alerts was to inform law enforcement personnel on issues pertaining to emerging technology and to provide guidance for investigations, where applicable. The first two NW3C cyber alerts uploaded to the LECC website addressed the applications Whisper and Discord. Whisper is a communication platform that enables users to post content and send messages without providing their identities (see National White Collar Crime Center, undated). Discord is a communication platform enabling voice calls, chat rooms, and other features, and has been identified as a distribution channel for hackers (see National White Collar Crime Center, 2017). Similarly, in 2016, the LECC website added National Consortium for Advanced Policing documents on cybersecurity and state and
local law enforcement, both as a news item on the site as well as part of the “IT Security Resources” webpage in the section of the LECC website targeting police chiefs (see Law Enforcement Cyber Center, undated[e]).
4. LECC’s List of Regional Capabilities Helped Link Crime Units

Development of Regional Capabilities List

The main effort under the objective of linking crime units was the development of a list of regional capabilities (i.e., local, regional, and national organizations, both private and government) that offer cyber-related services and assistance to law enforcement officials and prosecutors. The objective of the list was to help LECC website visitors identify and contact organizations, experts, and practitioners who could assist cyber-related investigations and prosecutions. The directory covered a variety of organization types, including cybercrime units, training facilities, fusion centers, and forensics labs.

The list of regional capabilities was continually updated as the project team collected new information. Originally, it was one long document on the LECC website. As described in Chapter Two of this report, to enhance the user-friendliness of the section, the project team introduced a search function for the regional capabilities list (see Law Enforcement Cyber Center, undated[c]).

The search engine enables searches to be performed by zip code, state, keyword, or areas of expertise. The options for topical expertise are:

- child exploitation
- community outreach
- computer and internet crime investigations
- counterintelligence
- critical infrastructure
- digital evidence and forensics labs
- education or training
- financial crimes
- incident response
- information sharing
- information technology security
- legal assistance
- research.

Users of the search engine have the option to click on individual search results, which will provide them with additional information collected on each organization. This information includes a detailed description of the organization in question, contact information, and more information on the organization’s capabilities, particularly those that were not covered by the original search. Users of the website are also offered the opportunity to provide feedback (e.g., if any information displayed is incorrect) and to contribute new content. The search interface is captured in Figure 4.1.
Over the duration of the project, the “Directory of Cybercrime Labs and Resources” section grew to include 1,007 entries, representing, to our knowledge, the most comprehensive directory of regional U.S. cybercrime labs and resources available. Since the launch of the website, the directory of cybercrime labs and resources page has had 1,303 page views from domestic users. Unfortunately, available data do not allow the team to comment on how many times the search engine was used or what visitors did with the retrieved information.5

5 Regarding the search engine method, this is because the URL after a completed search looks identical to when a user accesses the directory in the first place. In other words, if somebody runs a search, they will end up on the same page again.
5. LECC Developed Prevention-Focused Resources

Over the course of the project, LECC staff developed a series of materials in support of this task and made them available on the LECC website. There is a strong overlap between Task 2 (identify training and training gaps) and Task 4 (prevention education); as a result, most of the materials discussed under Task 2 are at least partially relevant for this chapter as well. However, several prevention-focused materials deserve particular attention.

The project team developed a prevention-dedicated section on the LECC website, titled “Cybercrime Community Awareness and Prevention” (see Law Enforcement Cyber Center, undated[b]). The webpage was intended as a resource for law enforcement responding to citizen reports or concerns around cybercrime. Accordingly, the webpage provides links to training modules and guides, as well as prevention brochures in various languages.
In addition, the LECC website also includes a series of education materials designed to assist law enforcement agencies in their own cybersecurity arrangements. One such item was a Chief’s Checklist (see Law Enforcement Cyber Center, 2015), a tool allowing agencies to better understand critical issues related to securing their information technology networks, identifying weaknesses, and using the materials available on the LECC website to take action to prevent cyberattack. Another item was a Cyber Report Card for police executives, developed in collaboration with the Canadian Association of Chiefs of Police, the CCDE Committee of IACP, chiefs of small- and mid-sized agencies, and LECC strategic partners (see Law Enforcement Cyber Center, undated[g]). The Report Card was intended to help police executives and their information technology departments to build and maintain robust information systems by offering a measure for an agency to evaluate its capabilities and protections in areas ranging from password and account management to policy and procedures and providing references to
more sources of relevant information available on the LECC website (see Law Enforcement Cyber Center, undated[f]). A third item was an article and infographic on the life cycle of a typical cyberattack and its individual stages (see Law Enforcement Cyber Center, undated[a]). Together, these resources were intended to contribute to the strengthening of the understanding and prevention of cyber-related issues by law enforcement agencies.

The LECC also coordinated with and supported external ongoing education campaigns. For instance, in July 2017, representatives of the LECC attended a White House meeting related to the education campaign “Lock Down Your Log In,” which focused on website authentication and using passwords to objective of reducing cyber intrusion and cybercrime. Following the meeting, the LECC project team provided information about the educational campaign in the “Chiefs Corner” on the LECC website. In another example, in October 2016, the LECC, in collaboration with DHS, cosponsored the National Cybersecurity Awareness Month. Each week of the campaign focused on a different cybersecurity issue, with its third week dedicated to combating cybercrime. Correspondingly, the LECC website featured special materials relating to the topic.

Prevention was one of the objectives of a very popular cyber alert on the LECC website in July 2016: “Pokémon Go: A Law Enforcement Alert” and an accompanying video. The video explained the Pokémon Go application and its potential effect for law enforcement. The video was one of the most popular items on the LECC website, generating more than 2,000 views.

Activities discussed elsewhere in the report were also relevant for this task. For instance, news items selected for inclusion on the website (see Chapter Three for a description of the procedure) regularly reported on issues related to prevention and raising awareness. The objective of providing NW3C cyber alerts on the website (see Chapter Three) was also to disseminate information about and increase awareness of novel technologies that may be used to facilitate cybercrime activities. Prevention of cybercrime also features strongly in the report on the implementation of the Utah Model and the establishment of a successful cybercrime unit (see Chapter Six). Discussions at the Justice Executive Cyber Roundtable (see Chapter Seven) also served to identify best practices in, among other areas, cybercrime prevention.
6. LECC Report on the Utah Model Offered Technical Assistance

The main effort under this task was the development of an instructional document providing information on the creation of a successful cybercrime unit. The model selected for the study was the Utah Department of Public Safety (DPS), also known as the “Utah Model.” The rationale for this selection was the fact that the DPS represents a robust program that was established relatively recently and has undertaken a range of relevant activities, ranging from cybercrime investigations to cyber intelligence analysis to assessments of the effect of cybercrime on areas such as emergency management and critical infrastructure.

In the preparation of the report, the project team conducted a series of consultations with relevant stakeholders. These included interviews with DPS staff involved in the unit’s management and operations, as well as representatives of partner agencies forming part of the Utah State Cyber Intelligence Network, a local partnership established to tackle cybercrime (see Utah Department of Public Safety, 2014, p. 2). In addition to local stakeholders, the project team also conducted site visits and interviews with representatives of other cybercrime units and agencies across the nation. This group of agencies included the San Diego Computer Technology Crime High-Tech Response Team (CATCH), the state prosecutor of San Diego County, and the New York City Wellspring Cybercrime Unit.

Building on the information collected, the report provided a description of the challenges faced by DPS in the establishment of its cybercrime program and identified a series of lessons learned as well as promising practices. Among the lessons learned was that defining cybercrimes remained a major challenge and stressed that building trust with the private sector was crucial in improving agencies’ understanding of cybercrime. Accordingly, agencies looking to investigate and prosecute cybercrimes need to invest in educating their own staff and their partners. With respect to cyber investigations, the report noted that no agency possessed the resources to address cybercrime on its own, that cybercrime may be more time intensive to investigate than other major crimes, and that investigations may make personnel working on them vulnerable to personal attacks.

In addition, the report addressed a series of individual aspects associated with the operation of a cybercrime unit, notably resources, training, leadership, and interagency coordination. Promising practices related to these areas included prioritization of cases and leads on potential cybercrimes, collaboration with state legislatures on building support for the cybercrime program under development, rethinking existing criminal codes to take into account the effect of cybercrimes, and creating and testing a cyber incident response plan. Other promising practices addressed collaborations, partnerships, and working with the FBI, state information-sharing initiatives, and information sharing with the private sector. The information presented in the
report was intended as a resource for other state and local agencies that are in the process of establishing their own cybercrime units.

A draft of the report was submitted to the BJA for review in December 2016. The project team subsequently received and incorporated feedback received from the FBI and BJS, along with additional input from the state of Utah to prepare a final version. After review by BJA, the report was made available on the LECC website (see Bureau of Justice Assistance, U.S. Department of Justice, and Police Executive Research Forum, 2015).

In addition to the work on the Utah Model report, the Justice Executive Cyber Roundtable (see Chapter Seven) also represented an opportunity to disseminate technical assistance materials. This included materials from morning presentations and panel discussions. After the conclusion of the roundtable, the project team provided additional materials about the admissibility of electronic evidence to roundtable participants. The articles were written by one of the judges who participated in the roundtable and were distributed with the permission of Thomson Reuters, the publisher.
On March 29, 2017, the LECC team held a Justice Executive Cyber Roundtable, which brought together 27 practitioners who represented various stakeholder groups, including police executives, investigators, prosecutors, and judges (see Appendix C for a full list of participants). The objective of the meeting was to discuss the challenges and resources needed to improve and address the growth of cybercrime and digital evidence from the perspective of the various stakeholder groups. Because there are only a limited number of fora in which representatives of different types of law enforcement and judicial agencies participate and exchange views, the event was intended to contribute to an improved crossdisciplinary understanding of cybercrime-related challenges and to foster a dialogue across various stakeholder groups.

In preparation for the roundtable, the project team reached out to law enforcement members, judges, and prosecutors to solicit feedback on possible formats and topics of interest to ensure the relevance of the event to all stakeholders. After an assessment of the initial feedback, the project team developed an outline of the event that underwent subsequent iterations within the project team and in consultation with the BJA (see final full agenda in Appendix D). Prior to the event, the project team held a series of conference calls with individual stakeholder groups (i.e., law enforcement, prosecutors, and judges) to discuss ideas for the structuring of the event’s working sessions. The topics identified during these preparatory calls related to challenges in the investigation and prosecution of cybercrimes. Specifically, the challenges identified were: (1) ability to recognize all levels of digital evidence; (2) availability, accessibility, and uptake of training; (3) retention of trained personnel; (4) data integrity and storage of evidence; (5) chain of custody; (6) jurisdictional issues; and (7) protection of agencies’ own information systems. The list of challenges was included in participants’ briefing pack distributed at the beginning of the roundtable.

The Justice Executive Cyber Roundtable was a daylong event hosted at IACP’s headquarters in Alexandria, Virginia. Its program was divided into a series of morning sessions and afternoon working groups. The event’s morning agenda included a presentation on the admissibility of electronic evidence followed by a group discussion and two panel discussions moderated by the RAND project manager about obtaining overseas data for transnational cyber investigations and emerging social media trends and applications (apps). In the afternoon, participants were divided into three working groups with discussions facilitated by a moderator following a semistructured protocol. Members of these working groups were invited to identify key concerns, challenges, and best practices for cybercrime investigations and prosecution. Participants were also asked to suggest areas where the LECC could provide guidance, resources, or assistance. The event concluded with a plenary discussion of the main themes identified during the day.
Numerous topics addressed by participants concerned the ability of judicial and law enforcement members to recognize and understand all types of digital evidence. Key issues included criteria for admissibility, authentication considerations, and challenges law enforcement and investigators face in obtaining data from service providers, particularly with respect to overseas data. The discussion also touched on how to deal with the trend of “going dark” and on emerging trends in technology that could have implications for criminal investigations.

Participants at the event also noted that the criminal justice system tends to respond slowly to digital evidence and cybercrime in general. Examples of how this issue manifests itself include the increasing difficulty in all domains of handling and using digital evidence (e.g., recognition, seizure, preservation, analysis, reporting), as well as the proliferation of digital devices and data-storage capacities. The continuous development and emergence of new types of digital technology create challenges for prosecutors and judges in authenticating digital evidence for use at trial.

In summary, in line with the event’s objectives, the discussions at the roundtable resulted in the identification of key concerns and challenges for cyber investigation and prosecution that merit further discussion and consideration. These are summarized in Box 7.1.

**Box 7.1. Key Concerns and Challenges Identified at the Justice Executive Cyber Roundtable**

1. The “going dark” phenomenon (involving data that are unobtainable to law enforcement due to privacy concerns, encryption, and/or data stored in foreign jurisdictions)
2. Government protection of infrastructure
3. Law enforcement training and retention of subject-matter expert personnel
4. Resource and information sharing
5. Authentication and admissibility of evidence in prosecutions


After the roundtable, participants were contacted and thanked for their participation and contribution to the event’s discussions. The project team also circulated a list of attendees and their contact information to all participants and distributed additional materials on electronic evidence related to one of the morning sessions. This set of materials included a journal article about approaches to authenticating electronically stored information (ESI) coauthored by one of the roundtable participants, a practical note that discussed the process and standard for the authentication of ESI in federal courts in accordance with the Federal Rules of Evidence, and a reference chart summarizing methods most frequently used to authenticate various types of ESI.
8. LECC Complied with All Administrative Requirements

Reporting Arrangements

Throughout the project, the LECC team adhered to fixed reporting arrangements to BJA. The team (including BJA representatives) regularly held progress calls every two weeks. Notes from each meeting’s discussion were distributed to the project team and partners. Every month, the LECC project team compiled a progress report summarizing the main achievements and activities. Every six months, the project team submitted a semiannual progress report on the BJA Training Portal and the Grants Management System. The reports summarized the team’s accomplishments during the last reporting period, outlined plans for the next reporting period, and highlighted any particularly noteworthy accomplishments or lessons from the project. The semiannual reports also provided an opportunity to comment on the extent to which the project was fiscally and programmatically on track and whether any barriers were encountered over the course of the project. In addition to these regular reporting arrangements, the project team remained available for any ad hoc or unanticipated requests from BJA representatives.

Transition to NW3C

In April 2017, control over the LECC was transitioned to NW3C. Members of the project team worked with NW3C partners to coordinate a smooth handover in all pertinent areas, including the management of the LECC website, web analytics, ownership of LECC documentation, and regular reporting requirements. The transition was completed successfully during the reference period.
9. Conclusions and Recommendations

We provide these conclusions and recommendations:

The LECC met its objectives and completed all its planned tasks. As outlined in this report, the LECC project team delivered on all substantive tasks agreed on at the outset of the project. These included setting up the LECC website, identifying training and training needs for various stakeholders, contributing to better links among crime units, enhancing prevention education, and developing technical assistance materials for relevant audiences. In addition, the project team organized the Justice Executive Cyber Roundtable, which provided a unique forum to bring together police chiefs, judges, and prosecutors to address the fight against cybercrime. By delivering on all of its tasks, the LECC met its objective to provide assistance to local and state law enforcement in addressing cybercrimes and cyber threats.

The metrics employed by the project team demonstrated the usefulness for the type of services provided by the LECC. As the LECC web traffic data demonstrate, the content provided on the LECC website was successful in attracting traffic to the website. Furthermore, the volume of traffic visiting the website grew over time, suggesting that it is possible to attract new users and retain existing visitors by providing a continuously updated set of relevant information. Similarly, the presentation of the LECC and its website at various meetings, fora, and conferences received interest and enthusiasm, indicating a perceived need for such a resource among various stakeholders. The LECC’s resources were also designed to foster greater links among crime units; for example, the LECC team compiled a list of regional capabilities relevant for combating cybercrime, such as forensics labs or training facilities. The list was converted to a searchable database to enhance its utility for users. The database grew to contain 1,007 entries, representing, to our knowledge, the most comprehensive resource available for this type of information. In a major technical assistance effort, the LECC team developed a report on the implementation of the Utah Model of cybercrime prevention, summarizing lessons and best practices from the implementation of a new cybercrime unit in Utah. It was designed as a resource for other agencies that are in the process of or are contemplating establishing a cybercrime unit. The report is now available on the LECC website. The benefits of the LECC can extend beyond the provision of resources on the website, as exemplified by the positive response to discussions at the LECC-convened Justice Executive Cyber Roundtable.

Future endeavors to assist state and local law enforcement and prosecutors with cybercrime prevention, investigation, and prosecution should continue to broker the exchange of knowledge within and across law enforcement stakeholder groups. The LECC’s
experience with its function as a clearinghouse for cyber-related information demonstrates that, while there exists a substantial amount of relevant knowledge and resources, this information is frequently hard to localize and access and may be spread across a large number of sources. Furthermore, this knowledge may not always be made available or disseminated beyond its immediate owners, thereby preventing its robust use in the law enforcement community. This is particularly the case with respect to sharing knowledge across important stakeholder groups, thus ensuring that law enforcement understands the perspective and experience of prosecutors and judges. The LECC contributed to bridging gaps concerning cybercrime prevention, investigation, and prosecution in the state and local law enforcement communities. For example, the LECC turned a high-performing agency’s cybercrime unit experience into a compendium of best practices (e.g., Utah Model report) and provided a forum for discussions and exchanges of best practices among key law enforcement stakeholders (e.g., Justice Executive Cyber Roundtable).

The LECC was envisioned as an online portal and a clearinghouse of information, directing users to existing resources developed and managed by subject-matter experts, professional organizations, and government agencies. This report explained how the LECC has raised the awareness of cybercrime in the state and local law enforcement community and enhanced the education and capacity of state and local criminal justice and public safety agencies with respect to cyber threats and cybercrimes.
Appendix A. List of Delivered Training and Technical Assistances

Table A.1. List of LECC Training and Technical Assistances (TTAs)

<table>
<thead>
<tr>
<th>Deliverable Title</th>
<th>Program Area Subtopics</th>
<th>Date</th>
<th>Venue</th>
<th>Type of Agency</th>
<th>Target Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>IACP LEIM conference</td>
<td>Investigations</td>
<td>May 2017</td>
<td>St. Louis, Missouri</td>
<td>Federal, state, local</td>
<td>Courts, judges, law enforcement, legislators, prosecutors</td>
</tr>
<tr>
<td>Justice Executive Cyber Roundtable</td>
<td>Technology implementation</td>
<td>March 2017</td>
<td>Alexandria, Virginia</td>
<td>Federal, state, local</td>
<td>Law enforcement, prosecutors</td>
</tr>
<tr>
<td>CSX Cyber Security Brainstorm</td>
<td>Technology implementation</td>
<td>December 2016</td>
<td>Washington, D.C.</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Insider Threat: Risk Mitigation and Compliance</td>
<td>Technology implementation</td>
<td>November 2016</td>
<td>Odenton, Maryland</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>DHS New Administration Cyber Concerns and Priorities</td>
<td>Technology implementation</td>
<td>November 2016</td>
<td>Washington, D.C.</td>
<td>State, local</td>
<td>Federal law enforcement</td>
</tr>
<tr>
<td>Solarwinds Technology Briefing</td>
<td>Technology implementation</td>
<td>November 2016</td>
<td>Washington, D.C.</td>
<td>Federal, state, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Solarwinds Technology Briefing</td>
<td>Technology implementation</td>
<td>November 2016</td>
<td>Washington, D.C.</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Federal Trade Commission Fall Tech Series</td>
<td>Technology implementation</td>
<td>October 2016</td>
<td>Washington, D.C.</td>
<td>Federal, state, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>DOJ Attorney General’s Community</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>Washington, D.C.</td>
<td>Federal, state, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Policing Awards Ceremony</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>Ashburn, Virginia</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>National Industrial Security Program</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>Washington, D.C.</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Insider Training Conference</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>Washington, D.C.</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>National Cyber Security Awareness Month Keystone Event</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>San Diego, California</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Police Executive Research Forum Town Hall Forum</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>San Diego, California</td>
<td>State, local</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>IACP Annual Conference</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>Boston, Massachusetts</td>
<td>State</td>
<td>Administrators, legislators</td>
</tr>
<tr>
<td>National Governor's Association Conference</td>
<td>Cybercrime</td>
<td>October 2016</td>
<td>Boston, Massachusetts</td>
<td>State</td>
<td>Administrators, legislators</td>
</tr>
<tr>
<td>Event</td>
<td>Type</td>
<td>Date</td>
<td>Location</td>
<td>Participants</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Cyber Situational Awareness and Information Sharing Conference</td>
<td>Technology implementation</td>
<td>September 2016</td>
<td>Fairfax, Virginia</td>
<td>State, local Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Virginia State Police and University of Virginia Pilot</td>
<td>Cybercrime</td>
<td>July 2016</td>
<td>Charlottesville, Virginia</td>
<td>State Law enforcement</td>
<td></td>
</tr>
<tr>
<td>White House/DHS Cyber Education</td>
<td>Cybercrime</td>
<td>July 2016</td>
<td>Washington, D.C.</td>
<td>Federal Administrators, corrections professionals, federal justice, legislators</td>
<td></td>
</tr>
<tr>
<td>CJTFG, Meeting #3</td>
<td>Technology implementation</td>
<td>January 2016</td>
<td>Arlington, Virginia</td>
<td>State, local Law enforcement</td>
<td></td>
</tr>
<tr>
<td>IACP and LEIM Training Conference and Technology Exposition</td>
<td>Crime analysis, equipment, technology, facilities, investigations, other law enforcement</td>
<td>May 2016</td>
<td>Dallas, Texas</td>
<td>Local Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Attended Global Advisory Committee Meeting</td>
<td>Technology implementation</td>
<td>November 2015</td>
<td>Washington, D.C.</td>
<td>Federal, Federal justice</td>
<td></td>
</tr>
<tr>
<td>Digital Prosecutor Training</td>
<td>General jurisdiction/trial courts, other adjudication/courts</td>
<td>August 2015</td>
<td>Long Beach, California</td>
<td>State, local Administrators, federal justice</td>
<td></td>
</tr>
<tr>
<td>Criminal Intelligence Coordinating Council Meeting</td>
<td>Crime analysis, investigations</td>
<td>January 2016</td>
<td>Washington, D.C.</td>
<td>Federal Administrators, federal justice</td>
<td></td>
</tr>
<tr>
<td>IACP Annual Conference</td>
<td>Crime analysis, investigations, cybercrime</td>
<td>October 2015</td>
<td>Chicago, Illinois</td>
<td>State, local Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Meeting with Utah State Bureau of Investigation</td>
<td>Technology implementation, crime analysis; technology implementation, cybercrime</td>
<td>January 2016</td>
<td>Sandy, Utah</td>
<td>Local Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Meeting with Statewide Information and Analysis Center</td>
<td>Technology implementation</td>
<td>January 2016</td>
<td>Sandy, Utah</td>
<td>Local Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Task Team Meeting</td>
<td>Equipment, technology, facilities, investigations</td>
<td>January 2016</td>
<td>Sandy, Utah</td>
<td>Local Law enforcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>February 2015</td>
<td>Washington, D.C.</td>
<td>Federal, local Law enforcement</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix B. List of LECC Deliverables

### Table B.1. List of LECC Deliverables

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Target Audience</th>
<th>Program Area Subtopics</th>
<th>Completion Date</th>
<th>BJA Logo</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Center introduction, IACP president Richard Beary</td>
<td>Video/CD/DVD/podcast</td>
<td>Law enforcement, prosecutors</td>
<td>Crime analysis, equipment, technology, facilities, investigations, other law enforcement</td>
<td>February 2015</td>
<td>Yes</td>
<td><a href="http://www.iacpcybercenter.org/resource-center/videos/">http://www.iacpcybercenter.org/resource-center/videos/</a></td>
</tr>
<tr>
<td>LECC website</td>
<td>Websites</td>
<td>Law enforcement</td>
<td>Equipment, technology, facilities, investigations</td>
<td>May 2015</td>
<td>Yes</td>
<td><a href="http://www.iacpcybercenter.org">http://www.iacpcybercenter.org</a></td>
</tr>
<tr>
<td>LECC brochure</td>
<td>Fact sheet</td>
<td>Law enforcement</td>
<td>Equipment, technology, facilities, other law enforcement</td>
<td>September 2015</td>
<td>Yes</td>
<td><a href="http://www.iacpcybercenter.org/resource-center/promotional-flyer">http://www.iacpcybercenter.org/resource-center/promotional-flyer</a></td>
</tr>
<tr>
<td>Regional capabilities list</td>
<td>Publication</td>
<td>Law enforcement</td>
<td>Crime analysis, equipment, technology, and facilities, investigations, other law enforcement</td>
<td>October 2015</td>
<td>Yes</td>
<td><a href="http://www.iacpcybercenter.org/resource-center/regional-labs-and-agencies-search/">http://www.iacpcybercenter.org/resource-center/regional-labs-and-agencies-search/</a></td>
</tr>
</tbody>
</table>
Appendix C. List of Justice Executive Cyber Roundtable Attendees

Note: Order of names reflect the distribution list at the event.

Christopher W. Kelly
Director, Digital Evidence Laboratory
Office of the Attorney General, Boston, Massachusetts

Brendan McHugh
Deputy District Attorney
San Diego County District Attorney’s Office, San Diego, California

Patrick E. Beasley
Special Assistant Attorney General
Mississippi Attorney General’s Office, Jackson, Mississippi

Demian Ahn
Assistant U.S. Attorney
U.S. Department of Justice, Washington, D.C.

Patrick Muscat
Assistant Prosecuting Attorney
Wayne County Prosecutor’s Office, Detroit, Michigan

Lucy Thompson, Esq.
Past President
American Bar Association Section on Science and Technology, Alexandria, Virginia

Terry L. Sult
Chief of Police
Police Department, Hampton, Virginia

Robert Merner
Assistant Chief of Police
Seattle Police Department, Seattle, Washington
Michael Yu
Sergeant
Montgomery County Department of Police, Gaithersburg, Maryland

T. J. Smith
Chief, Media Relations Section
Baltimore Police Department, Baltimore, Maryland

Sharisse Smith
Detective
Baltimore Police Department, Baltimore, Maryland

David Kurz
Chief of Police
Durham Police Department, Durham, New Hampshire

The Honorable Jackson Lucky
Superior Court Judge
Riverside County Superior Court, Riverside, California

The Honorable Lillie Sanders
Circuit Court Judge
Adams County Circuit Court, Natchez, Mississippi

The Honorable Robert E. Morin
Superior Court Judge
D.C. Superior Court, Washington, D.C.

The Honorable Felix J. Catena
County Court Judge
Montgomery County Court, Fonda, New York

The Honorable Michael D. Mason
Circuit Court Judge
Montgomery County Circuit Court, Rockville, Maryland

Anne Beck Tokoph
Deputy Chief, Criminal Law Section
Matt Wright  
Special Agent/Program Manager  

Tyler Wotring  
Computer Crimes Section Supervisor  
National White Collar Crime Center, Fairmont, West Virginia

James Emerson  
Chief Operating Officer/Managing Director  
iThreat Cyber Group, Inc., Princeton, New Jersey

Michael J. Stawasz  
Deputy Chief for Computer Crime  
Computer Crime and Intellectual Property Section, Washington, D.C.

The Honorable Paul W. Grimm  
District Judge  
U.S. District Court for the District of Maryland, Greenbelt, Maryland

**Supporting Agencies**

David Lewis  
Senior Policy Adviser  
Bureau of Justice Assistance  
U.S. Department of Justice, Washington, D.C.

Betsy Self  
Program Manager  
International Association of Chiefs of Police, Alexandria, Virginia

Steven Legacy  
Senior Research Associate  
Police Executive Research Forum, Washington, D.C.

Karlyn Stanley  
Senior Researcher  
RAND Corporation, Arlington, Virginia
Appendix D. Justice Executive Cyber Roundtable Agenda

8:30–9:00 a.m.  Introductions and initial roundtable discussion: Domingo Herraiz, James Patrick McCreary, and Jim Emerson
• Review key concerns and challenges for cyber investigation and prosecution identified by participants prior to roundtable
• Discuss a current cyber-related “hot topic” briefly in roundtable discussion

9:00–10:00 a.m.  Admissibility of Electronic Evidence: The Honorable Paul Grimm
• Judge Grimm discusses the challenges of admissibility and authentication of electronic evidence and the impact on cyber investigation and prosecution
• Interactive questions and answers with roundtable participants

10:00–10:15 a.m.  Break

10:15–11:15 a.m.  Panel Discussion: Current Challenges in Obtaining Overseas Data for Transnational Cyber Investigations: Michael Stawasz, Brendan McHugh, and Anne Beck Tokoph
• Panelists provide an overview of current case law and processes for obtaining overseas data, and the impact on state law enforcement investigation and prosecution of cyber cases
• Interactive questions and answers with roundtable participants

11:15 a.m.–12:15 p.m.  Panel Discussion: Emerging Social Media Trends and Apps: Christopher W. Kelly, Matt Wright, and Tyler Wotring
• Panelists present emerging social media apps and trends, as well as challenges and best practices for investigation and prosecution
• Interactive questions and answers with roundtable participants

12:15–12:40 p.m.  Briefing on Facilitated Working Group Structure and Deliverable: Karlyn Stanley
• Divide roundtable participants into groups that include a judge, prosecutor, and police chief to discuss cyber challenges, resources, and possible best practices

12:40–12:45 p.m.  BJA Update: James Patrick McCreary
12:45–2:00 p.m. Lunch (on your own)

2:00–3:00 p.m. Facilitated Working Groups

3:00–3:15 p.m. Break

3:15–4:00 p.m. Participants Report Out and Discuss Findings of Working Groups

4:00–5:00 p.m. Participants Revisit Key Concerns and Challenges for Cyber Investigation and Prosecution, Identify Best Practices
  • Discuss how LECC can share best practices or guidance developed from roundtable with other stakeholders

5:00 p.m. Adjourn
Law Enforcement Cyber Center

Your online resource for help in combating cyber threats and cyber crimes

“The cyber threat—cyber espionage, cyber crime, and cyber terrorism—is an enormous and an exponentially growing threat.”

— James B. Comey
Director, FBI

Law Enforcement Cyber Center

The Law Enforcement Cyber Center was created to enhance the awareness, expand the education, and build the capacity of justice and public safety agencies in preventing, investigating, prosecuting, and responding to cyber threats and cyber crimes. The Cyber Center provides:

- An easily accessible link to the FBI Cyber Shield Alliance (CSA), which provides secure law enforcement access to sensitive information.
- An online resource for law enforcement, criminal justice, and public safety agencies that channels users to tools and resources that support investigation, prosecution, digital forensics collection and management, and information systems security.
- An online toolkit of resources, training, technical assistance, and information sharing to help agencies address evolving threats and crime, support the diverse needs of their individual communities, and build secure and resilient information systems and resources.
- Resources tailored to meet the specific and practical needs of law enforcement leadership, investigators, line officers, digital forensic examiners, technical support staff, and other practitioners.
- A broad range of resources, training, technical assistance, and research currently offered by partner organizations worldwide.

www.iacpcybercenter.org

This project was supported by Grant No. 2014-DQ-BX-1022 awarded by the Bureau of Justice Assistance. Points of view or opinions on this product are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

http://www.iacpcybercenter.org/resource-center/promotional-flyer
Law Enforcement Cyber Center

Cyber crime is one of the greatest threats facing our country, and it has enormous implications for national security, economic prosperity, and public safety. The challenges facing state, local, tribal, and territorial (SLTT) law enforcement include investigating a broad variety of cyber crimes and cyber threats by criminals, hackers, terrorists, and state actors. In addition to dealing with these threats, law enforcement also must build secure and resilient information systems to support its operations and to address the ever-growing volume of digital evidence and forensic investigations. Nearly every criminal incident today involves some form of digital evidence, and equipping officers with the knowledge, skills, and tools to lawfully seize and secure this evidence when appropriate is crucial. Moreover, ensuring the safety and security of law enforcement systems and technologies, which are increasingly mobile, is equally important. The Law Enforcement Cyber Center serves as a central clearinghouse and online portal, channeling users to established resources managed by government and professional organizations and subject-matter experts.

“Cyber crime is a global threat to the economic and physical security of all nations. Law enforcement organizations must be prepared to recognize and investigate these crimes.”

— Chief Richard Beary
University of Central Florida and IACP Past President

Key Cyber Center Resources

LECC Chief’s Checklist—This quick reference guide is designed to support law enforcement leadership in understanding the broad topics of cyber crime, specific action items to be addressed, and resources available to assist in these efforts.

LECC Cyber Report Card—This resource is an easy-to-understand questionnaire that walks officials through the critical elements agencies need to assess their current security profile and build robust, resilient information systems.

LECC Regional Labs and Agency Search—This comprehensive database enables law enforcement to quickly connect with cyber crime experts and practitioners across the United States by searching via zip code, state, keyword, or areas of expertise.

Incident Reporting—A recommended process for reporting cyber incidents that occur to a law enforcement network, private citizens, or companies.

For More Information
For more information or to contribute content, e-mail cyber@theiacp.org.

The IACP, the RAND Corporation, and the Police Executive Research Forum (PERF) developed the Center in partnership with the Bureau of Justice Assistance and with funding from the Program Manager, Information Sharing Environment.

www.iacpcybercenter.org

“Cyber threats are among the gravest national security dangers to the United States.”

White House press release, February 25, 2015

Issued 09/15  Rev. 07/16
References


Law Enforcement Cyber Center, “Cyber Attack Lifecycle,” webpage, undated(a). As of December 27, 2017:

Law Enforcement Cyber Center, “Cybercrime Community Awareness and Prevention,” webpage, undated (b). As of December 27, 2017:
http://www.iacpcybercenter.org/resource-center/cyber-victimization-training/

Law Enforcement Cyber Center, “Directory of Cybercrime Labs and Resources,” webpage, undated(c). As of December 27, 2017:

Law Enforcement Cyber Center, “Incident Reporting,” webpage, undated(d). As of December 27, 2017:
http://www.iacpcybercenter.org/resource-center/incident-reporting/

Law Enforcement Cyber Center, “IT Security Resources,” webpage, undated(e). As of December 29, 2017:
http://www.iacpcybercenter.org/chiefs/it-security/chiefs-checklist/

Law Enforcement Cyber Center, “LECC Cyber Report Card,” webpage, undated(f). As of December 27, 2017:

Law Enforcement Cyber Center, “Strategic Partnerships,” webpage, undated(g). As of December 27, 2017:
http://www.iacpcybercenter.org/about-the-cyber-center/partners/

Law Enforcement Cyber Center, “Cyber Crime Checklist for Police Chiefs,” 2015. As of December 27, 2017:

https://www.nw3c.org/docs/research/whisper-application.pdf