Critical Systems Protection (CSP): The US Secret Service's Tactical Cyber Capability for Securing Protectees

Austin Hyman, Brian Nussbaum, Mario Bencivenga and Zachary Rizzo

College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC),
University at Albany, Albany, NY, USA

Corresponding Author: Brian Nussbaum

padcyber@albany.edu

Abstract: This paper examines a largely unknown cybersecurity function within the United States Secret Service (USSS), that is separate and apart from its traditional cybersecurity mission in financial crime investigations. This program - Critical Systems Protection (CSP) – is instead focused on the Secret Service's protective mission and analyzes and secures the cyber environments of facilities and locations visited by the agency's protectees. Exploiting publicly available documents about CSP, this paper will document this unique organization that combines some of the highest profile issues in cybersecurity – operational and tactical level cybersecurity efforts, and the security of cyber-physical systems. Drawing on open-source information and government documents, this paper sketches out the CSP mission, its partnerships with other agencies and organizations, and some of the tools and other capabilities it has developed.

Keywords: Cybersecurity, Law Enforcement, Executive Protection, Cyber-Physical Systems

1. Introduction

In April of 2017, CBS News ran a report entitled *"Secret Service costs for Trump family protection continue to mount"* (Strickler, 2017). The article described several unusual expenses tied to protecting President Trump and his family. These expenses included travel and vehicle rentals, and other expenses that members of Congress (Strickler, 2017) and the Government Accountability Office (LaRose, 2017) were monitoring to assess their appropriateness. One particular expense stuck out enough that the CBS piece (Strickler, 2017), and one from the New Orleans Times Picayune on the same subject (LaRose, 2017), noted as unusual – the expenditure by the United States Secret Service (USSS) of \$64,000 on *"elevator services"* at Trump Tower. The idea that it is strange or inappropriate for expenditures to be made securing the physical - and especially cyber-physical systems – that high value Secret Service protectees use is to miss (or misunderstand) one of the rapidly growing and fascinating components of the Service's protective mission. The CBS piece notes *"A Secret Service official told CBS News that 'elevator inspection is one of many protective operational measures utilized by the Secret Service.'"* (Strickler, 2017) In fact, the Secret Service has rapidly expanded the cyber component of its protection mission in recent years, in large part through a program called Critical Systems Protection (CSP).

The United States Secret Service has long played an important role in federal cyber-crime and cybersecurity investigations, though with a narrower focus than an organization like the Federal Bureau of Investigation (FBI). While the FBI investigates many types of cybercrime – from espionage to sabotage to fraud to data theft – the United States Secret Service has focused predominantly on cybercrimes targeting the financial sector and industry. This owes to the agency's foundational focus on economic crimes (Bumgarner et al 2017), which - while lesser known than their high-profile protective mission - shaped their approach to cybercrime.

The Secret Service has run Electronic Crimes Task Forces (ECTFs) since the mid 1990s (NLECTC, 2000) in conjunction with other Federal partners, as well as state and local agencies (USSS, 2021); however, these task forces have traditionally hewn close to the agency's focus on financial cybercrime. In 2020, the ECTFs were merged with the Secret Service's Financial Crime Task Forces (FCTFs), to create a new series of Cyber Fraud Task Forces (CFTFs) (USSS, 2020). As of mid 2020, there were 42 CFTFs in the United States, and international ones in London and Rome (USSS, 2020). The Service reports that *"Together with our partners, the CFTFs stand ready to combat the full range of cyber-enabled financial crimes."* (USSS, 2020)

In addition to the focus on financial crime, there have been several other themes that have defined Secret Services cyber efforts. Partnerships have been key to their building cyber investigation capabilities. Sometimes these have been partnerships with state and local government agencies through various task forces, but there have also been partnerships with academic institutions like Carnegie Mellon (on cybersecurity) and the University of Tulsa (on mobile phone security) (Lemieux, 2011). The Secret Service has also tried to build up the capabilities of state and local partners, through efforts like the National Computer Forensics Institute (NCFI) –

“the nation’s only federally funded training center dedicated to instructing state and local law enforcement officers, prosecutors, and judges in cybercrime investigations.” (Gaskew, 2019)

2. The CSP Mission

2.1 Program and Function

The Critical Systems Protection program is a component of the United States Secret Service’s protective mission that utilizes specially trained agents to identify, assess and mitigate cyber risks (GAO, 2020; DHS, 2020; GAO, 2014; Clancy, 2015). The program is responsible for evaluating cybersecurity threats to people, places and events protected by the USSS (DHS 2017; Clancy, 2015; Cybersecurity, 2013). The goal of the CSP is to strengthen the USSS’s protective operations by analyzing how information networks may impact the physical security plan or cause physical harm to the protectee (CERT, 2008; DHS, 2008). Additionally, the CSP is responsible for developing practical mitigation strategies that minimize the risk posed by these cyber impacts and prevent adverse impacts on protection (CERT, 2008, DHS, 2008). That is, the program leverages many of the skills and techniques that Secret Service agents and analysts bring to bear on traditional cybercrime, but does so not for financial criminal investigations, but rather to help protect the government officials and other high-profile targets that the Service is charged with protecting.

Operationally, the CSP relies on the expertise of its agents working in the Office of Investigations and external partnerships to secure the cyberspace surrounding protectees. The capability of investigative agents, especially those working on ECTFs or now CTFs, to conduct network monitoring and tracking are used in protective operations as a part of CSP advances (Goldstein, 2016; GAO, 2014). The CSP also works with partners inside and outside of the Federal government to develop tools, conduct research and increase capabilities (Sandia, 2019; DHS, 2013; CERT, 2008; SEI, 2002). In practice, the CSP is coordinated by agents in the Office of Investigations who are directed by a lead advance agent from the Protective Division. (GAO, 2020; DHS, 2011). The CSP typically deploys in advance of a protectee visit and coordinates with investigative agents from local field offices to conduct assessments and develop security plans (Senate Appropriations, 2017; Maui, 2017; Cybersecurity, 2013). During an event, dedicated CSP agents, and investigative staff are pulled from their normal duties, to monitor and respond to potential cyber threats to the operation or event, and to the protectee (GAO, 2020; DHS, 2019; Weiqun, 2017; Lowery, 2014).

Budget of Operational Mission Support (OMS) Initiatives (US Secret Service)						
	FY 16 Revised Enacted	FY 2017 Annualized CR	FY 2018 Request	FY 2019 Enacted	FY 2020 Enacted	FY 2021 Presidents Budget
Cyber Protection Activities Budget	\$6.3 million	\$6.3 million	\$6.3 million	\$6.8 million	\$7.002 million	\$8.2 million
Source	(DHS, 2018)	(DHS, 2018)	(DHS, 2018)	(Treasury, 2021)	(Treasury, 2021)	(Treasury, 2021)

2.2 Cyber Assessment of Protectee Visit Sites

The primary duty of the CSP is to conduct cyber assessments at venues and events where a protectee will spend time. Members of the CSP deploy in advance of protectee visits to conduct systematic audits and technical assessments of the sites where the protectee will be, as well as of the critical infrastructure and utilities that support the visit (Stegon, 2016; GAO, 2016; Clancy, 2015; DHS, 2011; Harlow, 2011). Advance assessments may begin as early as nine months pre-event to ensure that the CSP agents have identified and mitigated all potential cyber threats to the protective mission (Weiqun, 2017). CSP advance teams perform strategic assessments of the host city at the macro level to examine critical infrastructure and IT networks that may impact physical security. (DHS, 2019; Weiqun, 2017; Stegon, 2016; Clancy, 2015; DHS, 2011). According to Congressional testimony by former USSS Director Mark Sullivan, these assessments “*identify which computer networks, process-control systems, or remotely controlled devices could, if compromised, impact an operational security plan*” (Stegon, 2016). Agents also integrate and apply the latest threat intelligence to their operational security plans, collaborating with other members of the U.S. Intelligence Community to understand the current cyber threat landscape (GAO, 2014; GAO, 2020; Weiqun, 2017; USSS, 2013).

At the micro level, the CSP will assess the site where a protectee is visiting to mitigate risks to the actual facility. Advance teams evaluate buildings’ network infrastructure and IT systems to identify potential vulnerabilities

(Goldstein, 2016; GAO, 2020; Harlow, 2011). The methodologies employed by the CSP prioritize systems that may directly affect the safety of the protectee if disrupted or destroyed (GAO, 2020; Maui, 2017; GAO, 2014; CERT, 2008). Once vulnerabilities are identified, the CSP works with facility owners and operators to mitigate risks and protect their information systems (Goldstein, 2016; Maui, 2017). During the protectee's visit, CSP monitors networks and devices that could be compromised in-real time for potential breaches of security (GAO, 2020; DHS, 2019; DHS, 2013). At protected venues, agents ensure failsafe security controls are in place and are prepared to act in defense of IT networks in the event of malicious cyber activity (Weiqun, 2017; DHS, 2019).

Number of Advances Per Fiscal Year					
FY	FY 13	FY 14	FY 15	FY 16	FY 17
Number of Advances Per Fiscal Year	186	230	241	263	264
Source	(USSS Annual Report, 2013)	(USSS Annual Report, 2014)	(USSS Annual Report, 2015)	(USSS Annual Report, 2016)	(USSS Annual Report, 2017)

2.3 Cyber Assessments for NSSEs

In addition to protecting people, the CSP is tasked with protecting events designated as National Special Security Events (NSSEs). NSSEs are events designated by the Secretary of DHS or President of the United States that are of national significance and may be a target for criminal or terrorist activity (CRS, 2021). The USSS is the lead federal agency for developing and implementing security operations at NSSEs, of which cybersecurity is a critical aspect (DHS, 2019). The CSP has been involved with securing NSSEs since its inception, working to secure the 2002 Winter Olympics in Salt Lake City, Utah and 2002 Superbowl XXXVI in New Orleans, Louisiana (Lowery, 2014; SEI, 2003). The CSP scales its operations up to meet the needs of NSSEs, which are some of the most complex and logistically complicated protective operations undertaken by the USSS (DHS, 2019; Lowery, 2014). CSP employs very similar methodologies at NSSEs as it does for protective visits, working to identify and mitigate cyber risk at both the macro and micro levels (DHS, 2019; Stegon, 2016; Cybersecurity, 2013). The CSP has deployed to several NSSEs, including Presidential inaugurations, major international summits held in the U.S., major sporting events, and Presidential nominating conventions (CRS, 2021; Senate Appropriations, 2016; Weiqun, 2017; CERT, 2008).

2.4 Support to Other Missions

The CSP utilizes its expertise in cyber protection and risk mitigation to secure critical infrastructure in support of greater homeland security objectives (A. DHS, 2020). As a part of this effort, agents from CSP collaborate with critical infrastructure owners and operators to secure their systems from cyber threats (US Senate, 2013). CSP agents have conducted trainings with critical infrastructure stakeholders and local governments on the awareness of real-time network activity and the identification of malicious activity (DHS, 2013; DHS, 2008). In addition to this, CSP personnel have been requested to assist in assessing cyber threats to specific critical infrastructure facilities (US Senate, 2013). These assessments identify the critical components of a facility's cyber infrastructure and detail any potential vulnerabilities to them, as well as provide recommendations for mitigating those threats (US Senate, 2013). While details on specific CSP assessments of critical infrastructure operators are limited, its agents did conduct an assessment with a maritime port stakeholder in the Houston, Texas area and have engaged with similar stakeholders in California (US Senate, 2013).

3. Capabilities and Tools

3.1 Capabilities

While the full extent of CSP's capabilities is hard to judge based on publicly available information, the program has launched many hundreds of advance missions and has secured numerous types of events. In addition to the broader role of providing a cyber component to the protective mission, CSP has a number of narrower functions of importance. The CSP engages in training, software development, as well as representing the Secret Service at various types of events. Examples of such activities include:

3.1.1 Training

- Conducted training on the awareness of real-time network activity through traffic analysis and the identification of malicious network activity (DHS, 2013).

- Expanded the CSP program to 20 agents and increased capabilities to include a network operations center, R+D training and operation units (DHS, 2013).

3.1.2 Representation

- Represented the Secret Service and served as the sole presenter from the United States, at INTERPOL's request, in assisting the Government of Qatar in preparing for the 2020 FIFA World Cup (DHS, 2015).
- Collaborated with the Intelligence Community and private sector to support the State of the Union Address, the George W. Bush Presidential Center dedication, and the 68th United Nations General Assembly (DHS, 2013).

3.1.3 Technological Developments

- Developed and deployed a remote sensing platform with the Software Engineering Institute at Carnegie Mellon University (DHS, 2013).
- Conducted training on the awareness of real-time network activity through traffic analysis and the identification of malicious network activity (DHS, 2013)
- Successfully deployed the first full-time, USSS/CSP Liaison in partnership with the Executive Office of the President and the White House Communications Agency. This collaboration directly joins key forces in identifying cyber threats targeting USSS protectees and venues. This effort has enriched the threat information sharing platform and enhanced the cyber-security posture (DHS, 2016).
- Enhanced the CSP Program's Computer Network Defense mission by implementing sensors on a critical network managing energy delivery; thus, allowing the Service to proactively address cyber threats to its protective mission (DHS, 2016).

Research and Development Budget						
	FY 16 Enacted	FY 2017 Enacted	FY 2018 Enacted	FY 2019 Enacted	FY 2020 Enacted	FY 2021 Presidents Budget
CERT Program	\$250,000	\$250,000	\$250,000	\$250,000	\$1,750,000	\$250,000
Source	(DHS, 2018)	(DHS, 2018)	(DHS, 2018)	(Treasury, 2021)	(Treasury, 2021)	(Treasury, 2021)

3.2 Tools

Analysis of publicly available documents provides insight into the capabilities of CSP and the tools they use to conduct their mission. The CSP is currently using at least two major defense tools created by the Computer Emergency Response Team (CERT) at Carnegie Mellon University. These tools include the Kaleidoscope network defense platform and the Compass protective advance expert system application - formerly known as FlipBook (Treasury, 2021). *"CERT also developed the Bank Note Processing System (BNPS), which is an application that increased the efficiency of processing counterfeit bank notes in Secret Service field offices."* (A. DHS, 2020) CERT is not the only organization designing special tools and applications for CSP. The Tamizar tool, initially designed by Sandia National Lab for the U.S. Army, has become the primary network forensics tool for CSP (Sandia, 2019). The USSS relies on Sandia capabilities and expertise as part of a long standing and successful partnership. (Sandia, 2019). CSP has partner with other organizations to develop their tools, according to the US Secret Service yearly report in 2015 *"Partnered with two federally funded research and development centers, in developing customized tools to enrich the CSP Program's Network Traffic Analysis."* (DHS, 2015).

4. Partnerships

4.1 University, Research, and Analytical Partnerships

The Secret Service has recognized that partnerships are an integral part of both its investigative and protective missions (Maui, 2017). At the turn of the century, when the rise of cybercrime became more prolific, the USSS reaffirmed its commitment to work together and leverage relationships through its Critical Systems Protection Program (CSP) (Maui, 2017). The first of these partnerships began in 2001, with the collaboration of the U.S Secret Service and CERT at Carnegie Mellon (USSS, 2008). Through this partnership, the Insider Threat Study (ITS) was produced (USSS, 2008). Employing many of the same research methods as the Exceptional Case Study Project conducted by the USSS in 1977, the ITS focused on identifying information that may have been noticeable before an incident *"from both a behavioral and technical perspective"* (Harlow, 2001).

However, the collaboration between CERT at Carnegie Mellon and the U.S Secret Service would progress further, resulting in the creation of the Critical Systems Protection program. This initiative was designed to analyze the relationship between critical information networks and physical protection activities (SEI, 2003). Often used to support law enforcement, CSP was developed through the support of events such as the 2004 Olympic games, 2005 Presidential inauguration, and 2005 Olympic Games (CERT, 2008). When CSP is employed, often building owners and operators are worked with to ensure a building's cybersecurity is satisfactory (Goldstein, 2016).

Within two years since the start of this collaboration, Secret Service electronic crimes experts testified that this effort was “truly groundbreaking” in its ability to combine both the physical and cyber aspects of the Secret Service’s protective mission (USSS, 2003). In 2011, CSP once again utilized the resources of CERT, as well as adding both Carnegie Mellon University’s CyLab and Center for Sensed Critical Infrastructure Research (CenSCIR) to their collaborative effort (DHS, 2011). This partnership sought to create additional resources to further monitor critical infrastructure, systems, as well as a wide range of physical, cyber, and environmental threats (DHS, 2011).

However, Carnegie Mellon University has not been the only long-term partnership CSP has formed. Sandia National Laboratories has been a key contributor to the program for both its software development and cyber protection capabilities. In addition to the Tamizar software, Sandia Laboratory provided additional cyber support to the Secret Service (Sandia, 2019). In 2019, Sandia Laboratory was called upon by the USSS to provide “*onsite and remote cyber analysts*” for President Donald Trump’s State of the Union address, being one of only two agencies tasked with this mission. (Sandia, 2019). Sandia Laboratory has called this relationship “a long-standing and successful partnership.” (Sandia, 2019).

4.2 State, Local, Tribal, and Territorial (SLTT) Partnerships

Yet not all CSP’s partnerships are created with the intent of developing new tools or or analytic methodologies. Some, like the collaboration between the Maui County Police Department and USSS, are formed to leverage each other’s assets and capabilities. This example of a federal-local partnership was formed in 2017, with the USSS and Maui County Police department signing an intergovernmental agreement to enable joint operations and help organize the funding of such collaborations (Maui, 2017). The need for this agreement was born from the increase in “*network intrusion, malicious software, and unauthorized use of personal identification information*” in the region (Maui, 2017). To mitigate and deter these activities, the Secret Service provided a small team of specialized agents trained in network intrusions as well as Critical Systems Protection (Maui, 2017).

Beyond the level of counties, municipalities have also partnered with the CSP. The City of Beverly Hills is one of these partners (Beverly Hills, 2010). In 2010, the City of Beverly Hills Hazard Mitigation Action plan sought to conduct an assessment and analysis of critical infrastructure areas (Beverly Hills, 2010). The goal of this assessment was to observe how areas interfaced with physical and cyber components would be affected in a potential terrorist attack (Beverly Hills, 2010). To conduct this assessment, the city recommended utilizing the Secret Services’ CSPI (Beverly Hills, 2010). In 2016, a similar assessment was recommended (Beverly Hills, 2016). This time, the project focused on city facilities, including a metro line assessment. Once again, the use of CSPI was employed (Beverly Hills, 2016).

5. Conclusion

The Critical System Protection program within the United States Secret Service is a pioneering, and largely unknown program in the world of cybersecurity. This despite it being at the nexus of two of the most exciting and emerging cybersecurity issues – the first is that of securing cyber-physical systems, and the second is the idea that there can be some kind of “tactical” or “operational” cybersecurity that occurs in real-time as opposed to focusing just on cyber hygiene and the implementation of frameworks of controls. Without much fanfare, the Secret Service conceived of, built, funded, and operationalized just such a tactical cybersecurity function with a focus on operational technology and cyber-physical systems to bolster the security of its protectees. In most of cybersecurity, the asset being protected is data. In the world of Critical Systems Protection, their crown jewels really are High Value Targets.

References

- Bumgarner, J. Crawford, C. Burns, R. (2017) Federal Law Enforcement: A Primer. Carolina Academic Press.
- CERT. (2008). *CERT Research Annual Report 2008*. Carnegie Mellon, Software Engineering Institute. Retrieved from: https://resources.sei.cmu.edu/asset_files/CERTResearchReport/2008_013_001_54241.pdf

- City of Beverly Hills. (2010). Hazard Mitigation Action Plan: 2010-2015. Retrieved from http://www.beverlyhills.org/cbhfiles/storage/files/filebank/10286--9a_HazardMitigationPlan%201152011.pdf
- City of Beverly Hills. (2016). Hazard Mitigation Action Plan: 2016-2021. Retrieved from [http://www.beverlyhills.org/cbhfiles/storage/files/1388644851974314648/BeverlyHillsFinalHMP\(002\).pdf](http://www.beverlyhills.org/cbhfiles/storage/files/1388644851974314648/BeverlyHillsFinalHMP(002).pdf)
- Congressional Research Service. (2021). *National Special Security Events: Fact Sheet*. Prepared for Members and Committees of Congress, CRS Report R43522. Retrieved from <https://fas.org/sgp/crs/homesecc/R43522.pdf>
- Department of the Treasury, United States Secret Service. (2021). *Congressional Budget Justification and Annual Performance Plan and Report*. FY 2021. Retrieved from <https://home.treasury.gov/system/files/266/15.-USSS-FY-2021-CJ.pdf>
- Gaskew, B. (2019). Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget. Third Way. Retrieved from <https://thirdway.imgix.net/pdfs/override/Memo-Readers-Guide-Cyber-Budget.pdf>
- Goldstein, P. (2016). GITEC 2016: Cybersecurity complexity will Increase; Secret Service official says. *FedTech Magazine*. Retrieved <https://fedtechmagazine.com/article/2016/04/gitec-2016-cybersecurity-complexity-will-increase-secret-service-official-says>
- Harlow, R. (2011). *Two Missions, One Secret Service: The Value of The Investigative Mission* (pp. 1-85). [Master's thesis, Naval Postgraduate School]. Monterey, California: Naval Postgraduate School. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a552250.pdf>
- Innovation Law Lab, et al., v. Kirstjen Nielsen, et al., 3:19-cv-00807-RS. (United States District Court Northern District of California). 2019. Retrieved from <https://egov.gov/office-locator/#/asyresults/CA/California>
- LaRose, G. (2017) Trump family Secret Service costs piling up: report. *Times-Picayune*. April 14. Retrieved from https://www.nola.com/news/politics/article_3c5ab78a-c293-5df4-b88f-afab14f11961.html
- Lemieux, F. (2011). Investigating cyber security threats: Exploring national security and law enforcement perspectives. *2011 Developing Cyber Security Synergy*, 63.
- Lowery, E. W. (2014). *Closing the cyber gap: integrating cross-government cyber capabilities to support the DHS cyber security mission*. [Master's thesis, Naval Postgraduate School]. Monterey, California: Naval Postgraduate School. Retrieved from <https://www.hsdl.org/?view&did=762425>
- Maui County Government. (2017) A Bill For An Ordinance Authorizing The Mayor of The County of Maui to Enter Into An Intergovernmental Agreement With The United States Secret Service (USSS) Regarding Payment of Expenses from Joint Operations Between USS and The Maui Police Department, Bill #81, 2017. Retrieved from <https://www.maui-county.gov/DocumentCenter/View/110670/Ord-4772>
- National Law Enforcement and Corrections Technology Center (NLECTC). (2000). *Catching the Cyber Crook*. Retrieved from <https://www.ojp.gov/pdffiles1/nij/nlectc/211823.pdf>
- Report on 2017 Department of Homeland Security Appropriations Bill, 114th Congress, U.S. Senate, Committee on Appropriations (2016). Retrieved from <https://www.congress.gov/114/crpt/srpt264/CRPT-114srpt264.pdf>
- Sandia National Laboratories. (2019). *Labs Accomplishments: National Security Programs*. Sandia LABNEWS. Retrieved from https://www.sandia.gov/news/publications/lab_accomplishments/articles/2019/national_security_programs.html
- Software Engineering Institute. (2003). *SEI Annual Report FY 2002*. Carnegie Mellon, Software Engineering Institute. Retrieved from <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=30178>
- Statement of Director Joseph P. Clancy United States Secret Service Department of Homeland Security, 114th Congress, U.S. House of Representatives, Before the Committee on Oversight and Government Reform. (2015). Joseph P. Clancy. Retrieved <https://docs.house.gov/meetings/GO/GO00/20150324/103244/HHRG-114-GO00-Wstate-ClancyJ-20150324.pdf>
- Stegon, D. (2016). Secret Service Director Testifies on FY13 Budget. *FedScoop*. Retrieved from <https://www.fedscoop.com/secret-service-director-testifies-on-fy13-budget-1/>
- Strickler, L. (2017) Secret Service costs for Trump family protection continue to mount. *CBS News*. April 14. Retrieved from <https://www.cbsnews.com/news/secret-service-costs-for-trump-family-protection-continue-to-mount/>
- United States Department of Homeland Security, United States Secret Service. (2008). *United States Secret Service Strategic Plan* (FY 2008-2013). Retrieved from <https://www.hsdl.org/?view&did=487083>
- United States Department of Homeland Security, United States Secret Service. (2011). *United States Secret Service Fiscal Year 2011 Annual Report*. Retrieved from <https://www.secretservice.gov/>
- United States Department of Homeland Security, United States Secret Service. (2013). *United States Secret Service Fiscal Year 2013 Annual Report*. Retrieved from https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS_FY2013AR.pdf
- United States Department of Homeland Security, United States Secret Service. (2014). *United States Secret Service Fiscal Year 2014 Annual Report*. Retrieved from https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS_FY2014AR.pdf
- United States Department of Homeland Security, United States Secret Service (2015). *Fiscal Year 2015 Annual Report*. Retrieved from <https://www.secretservice.gov/sites/default/files/reports/2021-03/USSSAnnualReportFY2015.pdf>
- United States Department of Homeland Security, United States Secret Service (2016). *Fiscal Year 2016 Annual Report*. Retrieved from https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS_FY2016AR.pdf
- United States Department of Homeland Security, United States Secret Service (2017). *Fiscal Year 2017 Annual Report*. Retrieved from https://www.secretservice.gov/sites/default/files/reports/2021-03/CMR-2017_Annual_Report_online.pdf

- United States Department of Homeland Security, United States Secret Service. (2018). *U.S. Secret Service Budget Overview*. Retrieved from <https://www.dhs.gov/sites/default/files/publications/USSS%20FY18%20Budget.pdf>
- United States Department of Homeland Security, United States Secret Service. (2020b). *Office of Investigations Strategy Fiscal Year 2021-2027*. Retrieved from <https://www.secretservice.gov/sites/default/files/reports/2021-01/inv-strategy-fy21-27.pdf>
- United States Department of Homeland Security. (2019). *U.S. Secret Service Budget Overview: Fiscal Year 2019 Congressional Justification*. Retrieved from https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_CBJ-Secret-Service_0.pdf
- United States Department of Homeland Security. (2020a). *U.S. Secret Service Budget Overview: Fiscal Year 2020 Congressional Justification*. Retrieved from https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_CBJ-Secret-Service_0.pdf
- United States Government Accountability Office. (2014). *Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity* (GAO-14-459). Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate. Retrieved from <https://www.gao.gov/assets/gao-14-459.pdf>
- United States Government Accountability Office. (2016). *U.S. Secret Service Data Analyses Could Better Inform the Domestic Field Office Structure* (GAO-16-288). Report to Congressional Requesters. Retrieved from <https://www.gao.gov/assets/gao-16-288.pdf>
- United States Government Accountability Office. (2020). *Secret Service Investigation Operations Confer Benefits, but Additional Actions Are Needed to Prioritize Resources* (GAO-20-239). Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate. Retrieved from <https://www.gao.gov/assets/gao-20-239.pdf>
- United States Senate, Committee on Appropriations (2013) *Cybersecurity: Preparing For and Responding To The Enduring Threat*. 113th Congress, Committee on Appropriations. Retrieved from <https://www.govinfo.gov/content/pkg/CHRG-113shrg81526/html/CHRG-113shrg81526.htm>
- USSS. United States Secret Service (2003). *U.S. Secret Service Electronic Crimes Experts Address House Subcommittee on "Fighting Fraud: Improving Information Security"*. U.S. Secret Service Media Relations. Retrieved <https://www.secretservice.gov/press/releases/2003/04/us-secret-service-electronic-crimes-experts-address-house-subcommittee>
- USSS. United States Secret Service (USSS) Director's Update newsletter (2008) produced from January 1, 2001 to August 10, 2004. Retrieved from https://www.governmentattic.org/docs/USSSDirectorsUpdate_2001-2007.pdf
- USSS. United States Secret Service. (2020) *Secret Service Announces the Creation of the Cyber Fraud Task Force*. Retrieved from <https://www.secretservice.gov/newsroom/releases/2020/07/secret-service-announces-creation-cyber-fraud-task-force>
- USSS. United States Secret Service. (2021) *ECTF and FCTF*. Retrieved from <https://www.secretservice.gov/contact/ectf-fctf>
- Weiqun, Z. (2017). What does it take to (cyber)secure the presidential inauguration? *Federal Times*. Retrieved from <https://www.federaltimes.com/federal-times/2017/01/09/what-does-it-take-to-cyber-secure-the-presidential-inauguration/>