

Are federal security efforts evidence-based?

Cynthia Lum¹ · Breanne Cave^{1,2} · Jordan Nichols¹

© Macmillan Publishers Ltd 2017

Abstract Over the last few decades, local law enforcement agencies have become more receptive to incorporating research, evaluation, and analysis into their daily work, a concept known as “evidence-based policing.” Federal law enforcement and security agencies, in contrast, have rarely been evaluated and are traditionally much less open to input and analysis from outside researchers. Recently, leaders in the Federal Protective Service (FPS) have proactively pursued an evidence-based approach, looking to determine how research might apply to their mission and how partnerships with researchers can benefit their agency. In this study, we report on the first comprehensive “evidence assessment” of the deployment portfolio of the FPS. An evidence assessment is a translational criminology method which analyzes an agency’s practices and policies to ascertain how they align with existing crime prevention research. Our findings indicate that while some of FPS’s countermeasures are grounded in promising crime prevention measures, others are more uncertain. It is also unclear how some prevention strategies (such as guards and patrol) are used to optimize their effectiveness in evidence-based ways.

Keywords Federal Protective Service · Evaluation · Security · Evidence assessment · Translational criminology

This study was conducted through a U.S. Department of Homeland Security Contract to the RTI Corporation (HSHQDC-08-C-00100), through a subcontract to George Mason University (10-312-0211722). Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Homeland Security.

✉ Cynthia Lum
clum@gmu.edu

¹ Department of Criminology, Law and Society, Center for Evidence-Based Crime Policy, George Mason University, 4400 University Drive, MS 6D12, Fairfax, VA 22030, USA

² Present Address: Police Foundation, 1201 Connecticut Ave NW, Suite 200, Washington, DC 20036, USA



Introduction

Criminal justice agencies have become more open to conducting research, evaluation, and analysis as well as applying research outcomes to their daily work. In particular, law enforcement agencies are increasingly receptive to using knowledge gained from different types of research (e.g., evaluative, descriptive, analytic, surveys) and partnering with scholars to evaluate crime prevention tactics, managerial strategies, and internal policies. These activities are often described under an “evidence-based policing” framework, which advocates that agencies include scientific research and processes to inform decisions about reducing and preventing crime, improving community and citizen satisfaction, and increasing organizational functioning, competence, and professionalism (see Lum 2009; Lum and Koper 2017; Sherman 1998).

In U.S. law enforcement, evidence-based policing has been introduced and applied almost exclusively at the local level. For example, local police departments are the subjects of all of the evaluations in Lum et al.’s (2011a) *Evidence-Based Policing Matrix*, which holds the population of moderately rigorous to very rigorous policing evaluations on tactics to control crime. Eck’s (2002) review of security and situational crime prevention measures (see also Eck and Guerette 2012) is also dominated by evaluations of local-level strategies designed to block crime in stores, bars, parking lots, and the like. The National Research Council’s review of fair and effective policing (National Research Council 2004) reviews research conducted only on state, regional, and municipal law enforcement agencies.

Federal agencies are almost completely absent and immune from these evaluations and assessments.¹ Although these agencies develop and use a variety of law enforcement and security strategies, tactics, and programs that apply to borders, airports, federal facilities, and major criminal investigations, we are not aware of hardly any non-classified, rigorous, scientific evaluation of the effectiveness of a federal law enforcement strategy, tactic, or deployment. Many justifications may be offered for this lacuna of knowledge at the federal level (see Lum and Kennedy 2011). Some reasons are financial and practical. Funding for policing research by the National Institute of Justice, the Bureau of Justice Assistance, or private foundations primarily targets local law enforcement agencies, providing little incentive for researchers to focus their lens on the federal arena. Federal agencies are also not held accountable to local crime problems, making them less responsive to pressures from citizens or governments to innovate or evaluate.

But other reasons often reflect worries and suspicions that are reminiscent of policing research in the 1970s and 1980s. These include a lack of experience with research and researchers, a suspicion about the motivations of researchers, or a belief that research could reveal tactics, strategies, and enforcement weaknesses that may give offenders or terrorists the upper hand. Federal agencies can also be highly secretive and therefore lack transparency that is often demanded of their local

¹ Exceptions to this trend have been evaluations of metal detectors at airports, as well as the recent evidence assessment of the Transportation Security Administration (see Lum et al. 2011b).



counterparts. Data collected by federal agencies may be viewed as “secured sensitive information” (SSI) “classified,” or “for official use only” (FOUO) which must be carefully screened prior to release to researchers, or which prohibit researchers from publishing analysis of such data.² While some secrecy is warranted, the media, popular culture, and federal agents themselves have also created a mythology about a need for secrecy that can discourage scientific evaluation. As a result, federal law enforcement and homeland security agencies have remained at arm’s length from research and evaluation, a troubling state of affairs generally for democratic governance, and more specifically with regard to accountability of government spending and effective crime control and prevention.

Some federal agencies have recognized these concerns and are becoming more receptive to using social science to evaluate and justify enforcement and security tactics. This study is the result of such openness by one federal security agency—the Federal Protective Service (FPS), a large agency charged with federal building security. The authors were asked by the FPS and the Department of Homeland Security Science and Technology Directorate to conduct the first assessment of the evidence base of FPS’s security approach. The goal of this study was to comprehensively examine FPS’s security vision (countermeasures, risk and threat assessments) against what is known from research about similar types of prevention mechanisms. Such assessments are an important first step in laying the groundwork for understanding the nature of federal building security and setting the stage for both adjustments and evaluations of deployment tactics. While challenges remain (some materials in this study we can only generally discuss due to their FOUO status), the openness by FPS should encourage other federal agencies and researchers that increased evaluation, accountability, and innovation in federal law enforcement can be helpful in developing effective policies and practices.

The Federal Protective Service security tactics

The FPS is a federal law enforcement and security agency responsible for the physical security of more than 9000 federal facilities across the United States. These facilities are diverse in structure, location, function, and size, and range from highly visible and well-known federal government buildings to regional and local administrative offices, such as museums and national archives, clinics, and courts. The FPS describes its mission as “detecting, deterring, disrupting, and investigating threats using law enforcement authorities,” as well as to “protect critical infrastructure and ensure government continuity through a risk management process based upon Interagency Security Committee standards and the National Infrastructure Protection Plan.”³ The FPS’s primary customer is the General Services Administration (GSA).

The full history of the FPS will not be reviewed here, as it is provided by Reese and Tong (2010). However, events in the agency’s more recent history are relevant,

² This article itself was under legal review by the Department of Homeland Security for two years before the authors were granted permission to publish it.

³ See <http://www.dhs.gov/federal-protective-service>.



as they led to the development of its current security approach, which is analyzed in this study. After the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, President William Clinton established the Interagency Security Committee (ISC) on October 19, 1995,⁴ to address government-wide security standards for federal facilities.⁵ The committee included representatives from multiple executive branch departments (including the GSA) and was tasked with establishing and evaluating policies to mandate better practices for the protection of federal facilities (Reese and Tong 2010).

In 1995, the ISC drafted the first of several reports that would shape the strategic approach currently in place to prevent crime and terrorism at federal facilities—the *Vulnerability Assessment of Federal Facilities* report (United States Marshals Service 1995).⁶ This was the first report by the ISC to establish standards of security for the FPS to follow at federal facilities. Facilities were classified into five security levels ranging from low to very high risk, determined by their physical size and type (or function) and the number of employees they housed. The U.S. Marshals Service surveyed a sample of facilities to determine the types and costs of countermeasures in place among facilities with similar security levels. The report also “recommended minimum security standards applicable” at each security level (USMS 1995, pp. 2–5). These included 52 crime prevention measures (called “countermeasures”) for perimeter security, entry security, interior security, and security planning. For these 52 countermeasures, also referred to as “standards,” recommendations were made about the security effort appropriate to prevent crime in a facility given its assessed level of risk. These standards are further designated as “minimally required,” “desirable,” or “not applicable” based on the U.S. Marshals evaluation. From the documentation, it appears that these countermeasures, standards, and security-level determinations were established by gathering experts and using a consensus-based approach, as well as relying on a sample of facility observations conducted by the U.S. Marshals Service to inform decision making.

The Homeland Security Act of 2002 brought the FPS into the Department of Homeland Security under the Immigration and Customs Enforcement branch (ICE) (Reese and Tong 2010).⁷ In 2006, the ISC established the Existing Facilities Security Standards Working Group to “review and update the standards for existing facilities as set forth in the 1995 report” (ISC 2008). What emerged was the *Facility Security Level Determinations for Federal Facilities* report (ISC 2008).⁸ In this

⁴ See <http://www.gpo.gov/fdsys/pkg/FR-1995-10-24/pdf/95-26497.pdf>.

⁵ For more information on the ISC, visit <http://www.dhs.gov/about-interagency-security-committee>.

⁶ This report is publicly available from the National Criminal Justice Reference Service (see <https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf>) and therefore all information presented here does not violate any “secured sensitive information” or “for official use only” restriction.

⁷ In 2009, FPS was again transferred, this time from ICE to the National Protection and Programs Directorate (also under the Department of Homeland Security).

⁸ The report that was initially provided by the FPS to the researchers for purposes of this project was classified “For Official Use Only” (FOUO). However, this document is now superseded by a public document, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (ISC 2013a). All information presented here appears in that updated report (ISC 2013a) and is no longer protected.



report, the ISC expanded the security-level classification criteria to include five factors: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. Classification of a facility as low, medium, high, or very high risk was determined by the “Facility Security Level Determination Matrix,” which assigns points (from 1 to 4) for each of the five factors depending on specific aspects of each factor, and then tallies those points to assign each building a security level.⁹ This system takes a wide range of security threats into account, including common criminal acts. The 2008 report therefore provided more specific and quantitative criteria for determining the risk and security levels of federal buildings than the 1995 U.S. Marshals’ report. But like the Marshals’ report, the 2008 ISC report remained ambiguous about the underlying evidence supporting its assumptions regarding the appropriateness of the five factors used to categorize risk, as well as the criteria used to assess the number of threat-level points assigned.

In July 2011, the ISC developed the *Physical Security Criteria for Federal Facilities* report (ISC 2011). The 2011 report connects the risk assessments of facilities from the Facility Security Level Determinations report to specific countermeasures, thus developing more detailed security standards.¹⁰ To match countermeasures to identified risks, the ISC identified 86 security measures that could be implemented at any federal facility. These 86 measures appear to be an expansion of the 52 described in the 1995 report and include approaches that can be generally described as access control, control of the physical environment, prevention and protection measures within buildings, and the use of surveillance and screening technologies.

The 2011 report also detailed how each of the 86 security measures would be deployed given a building’s security level and its risk to adverse events. Rather than only denoting security criteria as “minimally necessary,” “desirable,” or “not applicable” as was done in the 1995 report, the 2011 report described a system in which each security measure escalates in a certain way according to a facility’s security level (or risk). For example,¹¹ one type of security criteria might be to control vehicle access into a building. Instead of indicating that this criterion was “desirable” for a building that was labeled as “low risk” or minimally necessary for higher risk facilities, the 2011 report specifies how countermeasures should escalate for each security level. For example, a low-risk facility might require no special measures for vehicle access, while a slightly higher risk facility may need special parking areas for visitors and employees. Buildings with even greater security risks might add gates, security barriers to limit access of vehicles, or armed guards at all

⁹ The point values and how they are derived are presented on pp. 4–16 of the updated ISC (2013a) report.

¹⁰ The report that was initially provided by the FPS to the researchers for purposes of this project was classified “For Official Use Only” (FOUO). This document is now superseded by the public document, *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (ISC 2013a). However, the appendix containing the countermeasures mentioned here and in the ISC (2013a) report remains FOUO, and is available upon request from and approval by the Office of the Interagency Security Committee at ISCAccess@DHS.gov. Because of this classification, no specific information about countermeasures from this report will be discussed in this paper, only general statements that are also discussed in the ISC (2013a) public report.

¹¹ This is a modified and general example given the “FOUO” classification of this document.



vehicle entrances. All of these measures could generally be defined as “controlling vehicle access,” but depending on the risk and threat to a facility, the manifestation of that measure could appear differently. In addition to providing more specific countermeasure descriptions and detailing the escalation of security measures for each facility security level, the 2011 document also described the events that each of the 86 countermeasures intended to prevent. In our stylized example, guards and barriers in a high-risk facility address the possible threat of a car bomb.

To supplement the 2011 report, the ISC produced the *Design-Basis Threat* report (ISC 2012).^{12,13} This report addressed how threat scenarios (for example, vandalism of a federal facility) might be matched with countermeasures (for example, officer patrols), and explained how the risk of any particular event was determined. The report also acknowledged the limitations of the prior sources of data used in making such determinations, stating that “more information was needed to support the evaluation of the threat as it pertains to the estimation of risk for each facility” and that “the methodology of incorporating the threat into the standards development process was inadequate and inconsistent. Previous documents developed the threat based solely on the knowledge of working group participants, without necessarily the expertise in, or availability of, intelligence analysis” (ISC 2012, p. 1).

The *Design-Basis Threat* report provides a more systematic approach to determining the threat posed by an undesirable event and identifies countermeasures that can prevent or mitigate that threat. As with previous reports, subject matter experts continued to be convened in a consensus-based approach to make these determinations. However, the ISC argued that the experts involved had “experience in developing and analyzing threat information and with access to the most current intelligence available were selected to participate in the document’s development” (ISC 2012, p. 2). Using past events and information, statistics, intelligence reports, and crime data, the report added empirical elements to justify threat assessments, providing further insight into how the ISC envisioned and calculated “threat” as well as the overall vision and expression of security as conveyed by ISC for FPS and federal facilities security.

In sum, these four reports document the evolution in the ISC’s vision and expression of security at federal facilities. This vision identifies undesirable events and their likelihood, assigns security levels based on facility risk as calculated by available information, and recommends scalable countermeasures that are believed to be effective given the type and nature of threats that federal facilities are likely to face. At the outset, our review of these documents raises important questions about the ISC’s security standards and policies. First, does their approach actually achieve optimal security at federal facilities? Are these approaches of matching risk,

¹² This report was initially provided by the FPS to the researchers for purposes of this project and was classified “For Official Use Only” (FOUO). This report remains classified as FOUO after the publication of ISC (2013a). Because of this classification, no specific information about countermeasures from this report will be discussed in this paper, only general statements that are also discussed in the ISC (2013a) public report.

¹³ According to the Department of Homeland Security, the most recent version as of the completion of this project is the 7th edition, published in March 2013 (also FOUO); the 5th edition was used for this project (<http://www.dhs.gov/interagency-security-committee-standards-and-best-practices>).



undesirable events, and countermeasures, as well as the countermeasures themselves, effective in preventing events? What is the basis for determining countermeasures and risk calculations? Such questions are relevant to many security and law enforcement agencies at the federal level, and recent GAO reports ask many of these same questions (see, e.g., GAO 2010, 2012a, b). However, because very little, if any, research is available about these interventions, the answers are often unknown. We now turn to a translational criminology methodology—evidence assessments—to approach these questions using research.

Assessing the evidence base of FPS security criteria and standards

There is no evaluation of the outcome effectiveness of FPS’s security criteria or countermeasures as described above, nor were we allowed to carry out such an evaluation. However, many aspects of the ISC’s security vision have parallels with criminological theories that attempt to explain crime and disorder (including terroristic crimes) as well as with evaluated crime prevention practices, which could provide clues as to whether FPS’s deployment strategy is likely to be effective.

Using existing research knowledge in a related field to estimate and appraise the effectiveness of a deployment portfolio not yet evaluated (or not able to be evaluated) is what is known as an “evidence assessment.” Evidence assessment is a translational criminology method first described for policing and security by Lum and Koper (2011) and Lum et al. (2011a) which uses visualizations and organizations of research evidence (such as the Evidence-Based Policing Matrix) to help determine the evidence base of a portfolio of tactics or strategies that have not been evaluated. Lum and Koper (2011) discuss it with regard to counterterrorism measures, while Lum et al. (2011b) applied it to a suite of interventions used by the Transportation Security Administration at airports. Gill et al. (2012) used the method to examine a number of crime prevention programs for the City of Seattle, while Veigas and Lum (2013) apply the approach to assess an entire local patrol deployment portfolio. The goal of an evidence assessment is not to provide definitive answers as to whether FPS’s security criteria at federal facilities are effective; only rigorous evaluation using sound scientific methods can attempt that. However, evidence assessments preliminarily help (1) examine whether interventions are grounded in theories supported by research, (2) determine the nature of existing interventions in their basic form (their “mechanisms of prevention”), and (3) assess whether those mechanisms have similarities to interventions already evaluated. In turn, these steps allow the assessor to critically appraise whether an agency’s deployment approach is aligned with what is known to be effective.

Evidence assessments can therefore identify misalignments between strategies and the totality of relevant evaluation research, stimulating discussion between agency and research partners about how an agency might strengthen its crime prevention and control measures. Knowledge from an evidence assessment helps suggest where more information, data, evaluation, and analysis are needed to better design an effective portfolio of countermeasures. We apply this approach at the request of FPS to specifically examine the ISC’s 86 security countermeasures as



well as more generally its security strategy as outlined by the documents mentioned above. Again, we note that because of the FOUO designation for the countermeasures appendix of the *Physical Security Criteria for Federal Facilities* and the *Design-Basis Threat* reports, we only discuss our results here in general terms, but have provided the FPS and the Government Accountability Office with the full reports, which are available to qualified parties.

Are the ISC's security measures grounded in evidence-based theories?

Like other agencies tasked with homeland security (for example, the TSA), the FPS protects federal facilities not only from terrorism, but also “everyday” crimes and disorders. This may be the reason why agencies like the FPS and the TSA (see Lum et al. 2011b) often use security measures that are very similar to common crime prevention strategies (Clarke and Newman 2006), some of which have been shown to be effective in preventing crime. In particular, many FPS security measures share general dimensions of situational crime prevention measures, like those developed by Ronald Clarke and his colleagues (see Clarke 1980, 1992, 1997; Cornish and Clarke 1987, 2003; for reviews of these measures, see Eck 2002; Eck and Guerette 2012). For instance, Table 1 shows an adaptation of Cornish and Clarke's (2003) 25 techniques of situational crime prevention, which are categorized into five general dimensions that characterize more specific crime prevention “techniques.” These general dimensions include interventions that increase offender effort, increase the risk of apprehension, reduce the rewards for offending, reduce provocations to offend, and remove the excuses for offending. Examples of techniques that could fall under each of these categorizations are wide ranging and can include hardening targets, identifying property, removing targets, setting rules, concealing targets, or conducting surveillance, to name a few. In practice, these strategies may include locking doors, erecting barriers, adding lighting, marking property, using closed circuit television (CCTV), deploying metal detectors, or controlling access to weapons, drugs, or alcohol.

Table 1 Cornish and Clarke's (2003) 25 techniques of situational crime prevention

Increase the effort	Increase the risks	Reduce the rewards	Reduce provocations	Remove the excuses
1. Harden targets	6. Extend guardianship	11. Conceal targets	16. Reduce frustration and stress	21. Set rules
2. Control access to facilities	7. Assist natural surveillance	12. Remove targets	17. Avoid disputes	22. Post instructions
3. Screen exits	8. Reduce anonymity	13. Identify property	18. Reduce emotional arousal	23. Alert conscience
4. Deflect offenders	9. Utilize place managers	14. Disrupt markets	19. Neutralize peer pressure	24. Assist compliance
5. Control tools/weapons	10. Strengthen formal surveillance	15. Deny benefits	20. Discourage imitation	25. Control drugs or alcohol

To view the full table with examples, see Cornish and Clarke (2003, p. 90)



Many of these techniques have theoretical and practical parallels to FPS's security measures. Because of this, Clarke and Cornish's typology provides a useful start to organizing some of the FPS countermeasures into more generalized descriptions, in which to assess their evidence base. It is important to note at the outset that the evidence for the effectiveness of these situational crime prevention measures is mixed (see Eck 2002), and not all of Clarke and Cornish's techniques in Table 1 have been evaluated using rigorous evaluation methods. Situational crime prevention practices are also meant to be specifically focused on the particular nature of the crime (see theoretical descriptions by Clarke 1980, and also Clarke and Felson 1993), which some might argue would make specific interventions less generalizable.¹⁴ FPS-related threats can also be as varied as crime and disorder, and existing crime prevention measures may not have anticipated all of these threats.

Despite these limitations, Clarke and Cornish's techniques are grounded in well-tested theories of rational choice and deterrence, opportunity, routine activities, and crime patterns/environment in which similarities to FPS security measures can be drawn. These theories examine how the immediate context or situation influences the likelihood of a criminal event rather than examine offender dispositions or the influence of macro social forces (i.e., poverty, employment, social disorganization) on the offender (Clarke 1980; Weisburd 2002). Rational choice theories (Cornish and Clarke 1986) suggest that given certain constraints, offenders (and people more generally) "respond selectively to...the opportunities, costs and benefits" associated with specific crimes (Cornish and Clarke 1987, p. 934; see also Berrebi 2009). Opportunity theory posits that offenders not only act rationally, but also take advantage of and seek opportunities to offend. Such opportunities present themselves in certain situations, physical structures, or routines of everyday human life and interaction (Clarke 1997; Felson 1994). Clarke and Newman (2006), Crenshaw (1990), and Dugan et al. (2005) have found that even seemingly irrational acts of terrorism are guided by notions of rationality, choice, and opportunity.

The FPS security standards also include elements of environmental, crime pattern, and routine activity theories. These theories posit that opportunities for crime are created by the convergence of routine activities in particular environmental contexts of potential victims, offenders, and guardians (Cohen and Felson 1979, 1993; Felson 1994; Sherman et al. 1989). Similarly, crime pattern theorists have asserted that the physical and social environment creates a context, backcloth, and "template" (Brantingham and Brantingham 1993) for crime that facilitates the attraction or generation of crime at specific places and locations. These theories are supported by many studies, including those focused on "crime prevention through environmental design" (CPTED) (see Cozens et al. 2005; Eck 2002; Jeffery 1971), hot spots research and problem-oriented policing at places (for general reviews see Braga et al. 2012; Sherman and Eck 2002; Weisburd et al. 2010), and studies related to environmental and geographic criminology.¹⁵

¹⁴ This important point was raised by one of the anonymous reviewers of this paper.

¹⁵ This list is too numerous to mention here, but includes scholars such as Anthony Bottoms, Kate Bowers, Anthony Braga, Paul and Patricia Brantingham, Joel Caplan, John Eck, Elizabeth Groff, Shane Johnson, Jerry Ratcliffe, George Rengert, Dennis Roncek, David Weisburd, and others.



Theories of deterrence are also relevant in assessing the evidence base for federal building security and are closely connected to rational choice, opportunity, situational, routine activities, and environmental theories. While both the certainty of apprehension and the severity of punishment are integral to deterrence policies and theory, research indicates that increasing the certainty and speed of apprehension and also heightening the risk of apprehension, even when an arrest is not made, are likely to be more effective as deterrents than the vague promise of more severe punishments in the distant future (Nagin 2013; Nagin et al. 2015). Like situational crime prevention approaches, deterrence strategies are underpinned by a rational choice and opportunity theory framework (Gibbs 1968; Nagin 1998; Tittle 1969), and many proactive, place-based, and tailored patrol activities have been shown to be effective (cf. Braga et al. 2012; Interagency Security Committee 2013a; National Research Council 2004; Sherman and Eck 2002; Sherman and Weisburd 1995; Weisburd and Eck 2004). A few of FPS's strategies focus on deterrence-based patrols and other proactive strategies.

Determining common crime prevention mechanisms of FPS security countermeasures

While noting the theoretical similarities between FPS's security vision and criminological theory is an important first step in an evidence assessment, the second step is more crucial: unpacking all of FPS's countermeasures to determine common crime prevention mechanisms and techniques, categorizing them according to some of these documented crime prevention mechanisms, and then applying this existing research knowledge back to FPS countermeasures. To start, the three members of the research team categorized each of the ISC's 86 security countermeasures according to Cornish and Clarke's (2003) 25 situational crime prevention techniques above. To do this, at least two members of the three-member research team assessed each security criterion separately to determine its placement into Cornish and Clarke's chart. The research team then met to discuss their coding and to settle discrepancies using a consensus-based approach with the lead researcher. The use of multiple coders and double-checking helped increase inter-rater reliability.

Table 2 summarizes the results of this classification process using the general descriptions provided by Cornish and Clarke. Notice that target hardening and access control are the security techniques most emphasized in the ISC's security criteria (26.7 and 18.6% of the 86 countermeasures, respectively). Countermeasures intended to strengthen formal surveillance (16.3%) are also common. Techniques appearing less frequently in the security criteria include controlling tools or potential weapons (5%), utilizing place managers such as guards (7%), reducing anonymity of potential offenders (6%), and concealing potential targets (5%). Rarely did the countermeasures attempt to increase natural surveillance, post instructions, deny benefits of the attacks, or screen exits, with only one criterion using each of these techniques. None of the ISC's security criteria attempts to "reduce provocations" for crime.

It is important to note that the frequency of a countermeasure's appearance in the ISC's criteria does not mean that any of these measures are *used* more or less frequently, but rather that they receive more or less attention from planners and subject



Table 2 Matching the ISC’s 86 security criteria/countermeasures with Cornish and Clarke’s 25 situational crime prevention mechanisms

Technique (as defined by Cornish and Clarke)	<i>N</i>	%
Increase the effort		
Harden targets	23	26.7
Control access to facilities	16	18.6
Control tools/weapons	4	4.7
Deflect offenders	3	3.5
Screen exits	1	1.2
Increase the risk		
Strengthen formal surveillance	14	16.3
Utilize place managers	6	7.0
Reduce anonymity	5	5.8
Assist natural surveillance	1	1.2
Reduce the rewards		
Conceal targets	4	4.7
Remove targets	2	2.3
Deny benefits	1	1.2
Remove the excuses		
Set rules	3	3.5
Assist compliance	2	2.3
Post instructions	1	1.2
Total	86	100

matter experts with regard to available options. Further, this first exercise alone does not confirm whether any of these tactics are effective. The classification of strategies only allows us to describe the overall makeup and tendencies of FPS’s security approach. To continue with the evidence assessment, we then examined existing evaluations of those prevention techniques for which FPS countermeasures could be associated. Using the findings from Table 2 as a foundation and guide, we further identified and grouped countermeasures according to common prevention techniques. In total, we identified 14 common strategies that appeared across the 86 security criteria. Again, to protect the FOUO classification of this document, we generalize our description of these prevention mechanisms into 10 items, and refrain from providing descriptions of four classifications that included such specific countermeasures that could not be generalized, except for metal detectors, which is a common and publicly known crime prevention strategy. These 10 techniques are as follows:

1. Crime prevention through environmental design/access control,
2. Security guards and preventative patrol,
3. Protection against gunfire and other weapons,
4. Alarm systems,
5. Employee training and codes of practice,
6. Closed circuit television (CCTV) and security in parking areas,



7. Regulatory signage,
8. Photo identification,
9. Lighting, and
10. Metal detectors.

Assessing the evidence base of FPS prevention security countermeasures

We then examined the existing evidence base for these 10 prevention techniques. To do this, we gathered all existing systematic reviews of evaluations of situational crime prevention measures (see Eck 1997; Sherman and Eck 2002; Eck and Guerette 2012) and also the Campbell systematic review on counterterrorism (Lum et al. 2006). We also used all of the data available from Lum et al.'s *Evidence-Based Policing Matrix*, which is an interactive online systematic review that provides all policing evaluations of crime control strategies of at least moderate rigor, updated yearly.¹⁶ Starting with existing reviews was important given a wide range of relevant evaluation research that could be applied to our ten prevention techniques and the extensive work already done by scholars to filter and rate studies by their methodological rigor, thus allowing us to use better quality studies in our evidence assessment. In addition to using these existing systematic reviews, we also searched academic databases for further studies not captured by these systematic reviews but that may speak to each of our categories listed above.

We caution readers that much of the evidence base for situational crime prevention measures has not employed highly rigorous evaluation designs, such as randomized controlled trials with larger sample sizes (Eck 2002; Sherman et al. 1997; Weisburd 2002). Many employ before–after designs or measure differences in the implementation of tactics in nonequivalent places or situations. Thus, findings from evaluation studies in this area may be considered less reliable (and also overly optimistic—see Weisburd et al. 2001) because of concerns of selection bias, violations of internal validity, and weak evaluation design. We also note that publication bias may be a limitation in our research; especially with situational crime prevention measures, unsuccessful evaluations may not have been published, which may lead to overly optimistic conclusions about particular crime prevention mechanisms (see further discussion by Rothstein 2007). Our findings for each of the ten strategies now follow.

Crime prevention through environmental design/access control

CPTED is a class of situational crime prevention that uses the physical environment to block or thwart opportunities for offending. Access control is one of the most frequently used CPTED strategies and was also the most frequently found prevention technique in the ISC security criteria (29.1% of the 86 countermeasures). Although the quality of scientific evidence regarding CPTED and access control remains generally low (tending to test interventions either with nonequivalent control groups or pre/post designs without a control group), many of these studies

¹⁶ See <http://cebcp.org/evidence-based-policing/the-matrix/>. See also Lum et al. (2011a).



have found promising crime reduction effects in targeted areas (see Eck 2002; Guerette and Bowers 2009). For example, Newman (1996) and Poyner (1991, 1994) found that design changes to restrict pedestrian movement were effective when deployed in residences and parking facilities. Atlas and LeBlanc (1994) as well as Lasley (1996) discovered that street closures were associated with less crime in surrounding areas. That is, crimes in many high-crime areas were caused by the permeability of the spaces to vehicle and pedestrian traffic, which were related to persistent prostitution and drug offending (see also Matthews 1993). Finally, Tilley and Webb (1994) found that providing locks and improved security in access points is effective in reducing burglary. CPTED is now a widely used approach in preventing crime; its promise suggests that including these types of countermeasures to improve FPS building security efforts is reasonable.

Security guards and preventative patrol

Security guards are a major part of the protection of federal facilities and appear in 15% of the security criteria. Security guards can provide general guardianship of federal facility space, security in high-risk areas, or preventative patrols throughout the space of an area. Research on the effectiveness of security guards in preventing crime in places has been promising, although evaluations have been moderate in rigor. Popkin et al. (1995), for example, found that the introduction of security guards in an apartment building resulted in a reduction of drug offending. Farrington et al. (1993) found that the use of security guards into retail stores resulted in a reduction of crime (see also National Association of Convenience Stores 1991). Security guards have also been linked to reductions in crime at banks and parking areas (Barclay et al. 1996; Hannan 1982; Hesseling 1995; Laycock and Austin 1992; Poyner 1994).

Directed patrol—and particularly problem solving in targeted locations—also has strong support in the evaluation literature. Policing research emphasizes that the location of law enforcement officers and how they conduct their patrols can make a significant difference in their ability to prevent and reduce crime and disorder (Braga et al. 2012). Combined with a large body of research that indicates crime and risk are highly concentrated in place (see Eck et al. 2007; Roncek 1981; Sherman et al. 1989; Sherman and Weisburd 1995) and that those concentrations remain stable over time (see Weisburd et al. 2004, 2012), this indicates that FPS can impact crime, disorder, and other security breaches through proactive, place-based, and targeted patrols (as opposed to random or reactive patrols). Deterrence by proactive security patrols can also be maximized, as Sherman (1990) and Koper (1995) point out, when patrols are conducted in high-risk areas and are unexpected, creating an uncertainty about when officers will be at any given high-risk location. Weisburd and Eck (2004), Lum et al. (2011a), and Weisburd et al. (2010) reviewed large bodies of policing research that points to the importance of tailored problem solving at places (see Eck 2002; Goldstein 1990), which can also increase the effectiveness of targeting certain high-risk locations. Finally, we know that directed patrols do not necessarily displace crime or offenders to other locations (Weisburd et al. 2006; Braga et al. 2012).



It is unclear from the ISC documents whether directed patrol is emphasized in training or deployment. Recently, ISC released *Best Practices for Armed Security Officers in Federal Facilities* (ISC 2013b),¹⁷ which provides the baseline standards for armed security officers. While directed patrol is implied in some of the tasks (e.g., task 4.07: “Patrol locations in areas which are potentially hazardous to the public [e.g., constructions sites],” p. A-2), a directed patrol approach is not explicitly emphasized. Rather, task 4.05 directs security officers to “Conduct patrols in accordance with routes and schedules contained in post orders” (p. A-2). We suspect that this directive is similar to a law enforcement patrol assigning beats and routes to create “omnipresence” over an entire area.

Blast/gunfire protection

The third most frequently appearing prevention mechanism in the ISC’s 86 security criteria was blast and gunfire protection, which is mentioned in 12 (14.0%) of the 86 countermeasures. This includes resistance measures designed to stop gunfire or explosive attacks on federal facilities. Although this type of countermeasure is rarely evaluated in criminal justice evaluation studies, parallels might be drawn to the use of bulletproof screens in reducing robbery as well as the fortification of embassies and protection of diplomats against attacks. With regard to bulletproof screens, moderately rigorous evaluations by Ekblom (1987, 1988) found that such barriers in front of clerks in post offices resulted in a 55–65% reduction in robbery (see also Clarke and McGrath 1990). In terms of the fortification of embassies and protection of diplomats, Lum et al. (2006) found four moderately rigorous studies that seem to suggest these approaches do not lead to significant reductions in terroristic events (Cauley and Im 1988; Enders and Sandler 1993, 2000; Enders et al. 1990).

Alarm systems

The use of alarm systems is the fourth most frequently appearing prevention mechanism in the ISC security criteria (11 of the 86 countermeasures). Alarm systems are primarily used for preventing entry into critical security areas during certain types of emergencies, detecting intruders in secure areas, and securing emergency exit doors. Evaluation research in crime policy has not often considered the effectiveness of alarms in preventing public injury or death in the case of emergencies, although weak evidence in emergency management evaluation research points to positive effects (see Istre et al. 2002; Simons and Sutter 2004). Some positive evidence employing weaker quasi-experimental designs in the area of preventing theft through electronic tagging of clothing, which activates alarms on store exits, may be relevant (see Bamfield 1994; DiLonardo 1996). However, using a rigorous quasi-experimental design, Crow and Erickson (1984) did not find

¹⁷ This document is publicly available at http://www.dhs.gov/sites/default/files/publications/Best%20Practices%20for%20ASOs%20in%20Federal%20Facilities%202nd%20Ed%20%20April%202013_508_0.pdf.



significant robbery reductions when evaluating the effectiveness of silent alarms and cameras at convenience stores.

Researchers have also found that while burglar alarms are associated with a reduction in burglary, there is not strong evidence of the effectiveness of the alarms themselves in preventing crime, and crime prevention outcomes are most often realized when alarms are used with a group of other interventions (Crow and Bull 1975; Tilley 1993). Sampson (2011) adds that the benefits of burglar alarms are counterbalanced by the costs associated with false alarms, which can take up a great deal of law enforcement time (see also Bennett 2003; LeBeau and Vincent 1997). Thus, it may not necessarily be the presence of the alarms that contributes to the effectiveness of this countermeasure. Rather, how alarm systems are implemented, monitored, maintained, and managed by FPS officers determines their potential effectiveness.

Employee training and codes of practice

Ten of the security criteria (11.6%) used employee training and codes of practice to prepare for and respond to incidents of crime or terrorism. These security criteria were primarily designed to detail responsibilities for specific individuals before, during, and after emergencies. Crime prevention research suggests that employee training and codes of practice can be effective in reducing crime and disorder. Much of this research, however, focused on training and codes of practice at bars (Felson et al. 1997; Homel et al. 1997; Putnam et al. 1993; Saltz 1987). As Sherman and Eck (2002) note, there is also support for the effectiveness of training in increasing the capacity of the police to detect concealed weapons and respond to domestic violence (see also Sherman et al. 1995). However, there are few direct evaluations of the effectiveness of particular management processes and training in reducing crime and disorder in workplaces (Runyan et al. 2000).

Closed circuit television (CCTV) and security in parking areas

The use of CCTV and security in parking areas appears in eight of the ISC's 86 security criteria. CCTV has a modest crime reduction effect according to a Campbell Collaboration systematic review of evaluation research of CCTV by Welsh and Farrington (2008a) and is most effective in preventing vehicle theft in parking lots (see also Sarno, Hough, and Bulos 1999). It is also effective when used in conjunction with other interventions such as additional security attendants and restricting access to parking areas (see, e.g., Barclay et al. 1996; Hesseling 1995; Poyner 1991, 1994; Tilley 1993). The crime prevention benefits of CCTV may persist for long periods of time. For example, Griffiths (2003) found that installation of CCTV in a town center in Gillingham, UK, was associated with a reduction of crime for a five-year period. As Ratcliffe and Taniguchi (2008) note, the crime prevention effects of CCTV may vary between locations depending on the nature of crime in those specific settings.



Regulatory signage

Five security criteria (5.8%) involved the use of regulatory signage. As described by Clarke (1997), regulatory signage informs the public of the rules for using spaces, emphasizes that spaces are being monitored by law enforcement or security personnel, or notifies the public of ongoing crime prevention or security interventions. Bowers and Johnson (2003) found that intense publicity about burglary reduction schemes is associated with a decline in burglary. Posting signs about CCTV have been linked to reductions in crime and disorder in places (Mazerolle et al. 2002; Tilley 1993). However, we were not able to locate evaluations that solely evaluated the effects of regulatory signage in isolation from other types of interventions and thus these conclusions are tentative.

Photo identification

Photo identification requirements are implicated in four of the 86 countermeasures. Relatively few studies have focused on the effectiveness of photo identification in crime prevention and security. However, existing studies support the notion that identification requirements can reduce crime and disorder. For instance, Popkin et al. (1995) found that issuing identification cards to residents of high-crime housing projects in Chicago (among other crime prevention measures) reduced subsequent violent crime. Masuda (1993, 1996) found that when convenience store clerks were provided with information about potential offenders, either through liaison with law enforcement or through requirements for photo identification, they were able to reduce credit card fraud.

Lighting and Metal detectors

Finally, lighting and metal detectors were common prevention mechanisms mentioned in the 86 criteria. A Campbell systematic review by Welsh and Farrington (2008b) as well as studies by Painter and Farrington (1997, 1999a, b, 2001) carried out primarily in the United Kingdom in residential areas show crime reductions in the treatment areas with increased lighting, as well as possible diffusion of crime control benefits to neighboring areas. Metal detectors remain one of the most evaluated counterterrorism measures and have been shown to be effective in reducing hijacking incidents (see Cauley and Im 1988; Enders et al. 1990; Enders and Sandler 1993; see also the review by Lum et al. 2006). This intervention appears once in the ISC security criteria, although we remind readers its appearance in the security criteria does not indicate how frequently this countermeasure is used.

The evidence base of other aspects of ISC's security approach for FPS

In addition to examining the evidence base of common crime prevention techniques within the 86 security countermeasures of the FPS, we also considered how research informs the determination of the types of threats that the security criteria are intended to address as detailed in the *Design-Basis Threat* report. An important part



of evidence-based approaches is not only reflecting on existing research, but also using relevant and high-quality data, information, intelligence, and the analysis of that information to guide decision making (Sherman 1998). Recall, the goal of the *Design-Basis Threat* report was to do just that—provide a more systematic approach to determining the level of risk and threat faced by a federal facility based on the possibility of undesirable events that may occur. Previous efforts had relied primarily on subject matter experts in the working groups, while the 2012 *Design-Basis Threat* report suggested the use of more empirical and analytical information.

For each possible type of threat anticipated against federal facilities as described in the 2011 report, the ISC assessed a baseline threat of minimum, low, medium, high, or very high in the 2012 document. (Again, we do not show the list of threats here due to the FOUO nature of this document.) Additionally, for each undesirable event, the committee detailed, in narrative form, how it derived this assessment of the baseline threat and determined the “attractiveness” of facilities for potential offenders as well as the outlook for improving countermeasures against a particular threat.

When examining each of these narratives, it remained unclear to what extent crime/intelligence analysis, intelligence reports, national data, and historical information contributed to the determination of the baseline threat or analytic basis. We use as an example a common crime problem mentioned in the ISC’s 2012 report—robbery. In determining the possibility of robbery at federal facilities, the ISC used national robbery figures, with aggregate crime reports cited from the Uniform Crime Reports of the Federal Bureau of Investigation by population level (all publicly available information). However, no statistics about the rates of robberies around federal buildings are presented or encouraged for use in determining whether the threat of robbery is “high,” “medium,” or “low” at any given federal building.

Overall, our analysis found that the assessment of threats against federal facilities still primarily focuses on anecdotal case studies, past events, and aggregate-level data. Indeed, anecdotal information appears in 71% of these narratives. National data were used in almost 26% of these descriptions, although those data are not specific to the federal facilities themselves. Other federal agency risk assessments appear in 16% of the narratives, and data from the FPS itself appear in only about 10% of the narratives designed to inform FPS countermeasures. However, both risk assessment data and FPS information seem necessary to establish a more systematic approach to determining the reality of threats to federal facilities (and relevantly, to determining their security levels), but they are the least used sources of information to determine the salience of any given threat.

Discussion and conclusion

Evidence-based policing has yet to permeate federal law enforcement and homeland security agencies as it has for some state, county, and local police forces. Thus, the Federal Protective Service’s interest in analyzing the evidence base of its security approach is unusual and innovative. Using a translational criminology method—



evidence assessments—we were able to take a “best guess” as to the evidence base of the ISC’s security approach for the FPS in the absence of being able to carry out an actual evaluation. Recall, such assessments (1) examine whether interventions are grounded in theories supported by research; (2) determine the nature of existing interventions in their basic form (their “mechanisms of prevention”); and (3) assess whether those mechanisms have similarities to interventions already evaluated.

With regard to (1), we found that the ISC’s security criteria were generally grounded in theories that have strong support in the criminological literature. These include deterrence, rational choice, opportunity, routine activities, situational, and environmental theories. In other words, the ISC’s expectations about how the FPS can accomplish security are appropriately anchored in theoretical approaches supported by research.

Unfortunately, theories supported by empirical testing do not guarantee that interventions built from those theoretical foundations will, in turn, be effective. For (2), we unpacked the 86 security criteria to determine common crime prevention mechanisms, examined the implementation of security (i.e., the escalation of those countermeasures for different building security levels), and explored narratives of how ISC determined the nature of both threats to facilities as well as factors contributing to risk. Through this holistic exercise, this part of the evidence assessment allowed us to unearth the prevention tendencies of the FPS’s security vision. Specifically, FPS tends to focus on hardening targets, increasing surveillance, and controlling access. However, additional approaches that might be useful to the FPS that are much less emphasized. These include reducing rewards (i.e., concealing or removing targets), removing excuses (i.e., setting clear rules, posting signage, controlling criminogenic commodities), or reducing provocations (i.e., reducing frustrations or stress, preventing disputes through policies, reducing emotional arousals). Knowing these tendencies of FPS’s security vision does not tell us about the effectiveness of these measures, but it does give a more holistic picture about the types of approaches used by the FPS, at the same time pointing out other options that might be used. It also provides researchers with a more specific description of federal security than has been previously available.

In terms of (3), assessing whether these interventions have evaluation support from existing research, the goal of the evidence assessment is to reduce the multitude of countermeasures to common approaches and then find parallels in the evaluation literature. Of the FPS strategies that could be directly compared to crime prevention interventions previously evaluated, we found that a number of interventions do have support from research evidence, albeit of modest quality. These include the use of metal detectors, lighting, CCTV, the posting of guards, and employee training.

However, the evidence assessment also produced a few additional lessons. The first is that FPS does use some countermeasures which are less supported by research, including blast/gunfire protection to prevent or discourage terrorism incidents, and alarms, which alone may not necessarily prevent attacks. Another example was the way FPS uses guards and patrol. Subsequent analysis of other publicly available ISC literature mentioned above indicates that guards may not be used in the most evidence-based ways to create the greatest deterrent effect (i.e.,



targeted and unpredictable patrols). Hence, the second lesson: how these measures are implemented on a daily basis (as well as how frequently) remains unknown, even to the FPS itself.

More generally, with regard to the final goal of evidence assessments, this process revealed that the ISC still relies a great deal on consensus-based decision making, using subject matter experts with a heavy reliance on past incidents and anecdotes as well as generalized, non-specific data to determine the risk of specific federal facilities. It remains unclear how internal or external conditions influence risk at specific facilities, how different security levels are derived from local calculations of risk, and how levels of security are linked to the implementation of security practices in specific places. This is not uncommon in many law enforcement arenas and is the challenge of evidence-based policing more generally. Neither research evidence nor a focused, data-driven approach appears to be “part of the conversation” (see Lum et al. 2012; Lum and Koper 2017) in ISC’s development of FPS’s security vision more generally or specific countermeasures. Even an analysis of its calls for service (or incident) data each year¹⁸ as well as crime data from local jurisdictions in which buildings were situated would be an important start to using more empirical information to guide decision making.

However, evidence assessments serve two purposes. First, it provides a model for federal law enforcement agencies like the FPS to move beyond anecdotal, consensus-based decision making and toward incorporating research and data-driven approaches in both strategic and tactical decision making. For example, FPS officials could conduct regular meetings discussing and documenting which countermeasures are used most often and why, reflecting on knowledge from related evaluation research as well as internal data (as suggested by Sherman 1998). Such assessments might also spark motivation to begin developing measures of frequency of use of specific tactics, and more understanding about how strategies are deployed. Discussing effectiveness of interventions could also prompt the development and collection of potential measures of effectiveness (for example, reductions in calls for service, crime, disorder, or violations of regulations) so that efforts could be evaluated.

The second purpose of this evidence assessment is to increase awareness of the challenges of translating research into practice for an agency like the FPS. No single action by the FPS or ISC can achieve the goal of more evidence-based federal facility security. Rather, an infrastructure for evidence-based security must be developed to support this type of approach (Lum and Kennedy 2011). Building this infrastructure requires developing clear standards for the reporting, recording, automation, and analysis of security incident data at each of the nation’s federal facilities. Goals could also include engaging in regular, consistent, and systematic analysis at each facility to understand specific threats for each facility as part of its risk assessment. Establishing strong and formal partnerships between the federal facility managers and the law enforcement jurisdictions where that facility is located can also help generate environmental or spatial data that could be used to better

¹⁸ See <http://www.dhs.gov/topic/federal-protective-service>, which describes the FPS as handling 534,000 calls for service each year.



calculate risk and threat for any given facility. Performance measures related to the implementation of security criteria at the local level must also be collected in order to determine how countermeasures are being delivered in relation to risks at that particular location. Further, a culture of research and evaluation should be normalized and institutionalized into the agency, including the hiring of security and crime analysts and statisticians and openness to subject matter experts in the area of crime prevention.

A number of law enforcement agencies have gained value and cost effectiveness from using evidence-based approaches and paying more attention to research. Many local police agencies now have crime analysis units that can analyze specific trends relevant to risks in their jurisdictions, as well as apply effective crime prevention principles based in research knowledge. The FPS's interest in learning more about these approaches is an important step forward.

References

- Atlas, R., and W. LeBlanc. 1994. The impact of street closures and barricades: A Florida case study. *Security Journal* 5 (3): 140–145.
- Bamfield, J. 1994. Electronic article surveillance: Management learning in curbing theft. In *Crime at work: Studies in security and crime prevention*, ed. M. Gill, 155–173. Leicester: Perpetuity Press.
- Barclay, P., J. Buchley, P.J. Brantingham, P.L. Brantingham, and T. Whinn-Yates. 1996. Preventing auto theft in suburban Vancouver commuter lots: Effects of a bike patrol. In *Preventing mass transit crime, crime prevention studies*, vol. 6, ed. R.V. Clarke, 133–161. Monsey: Criminal Justice Press.
- Bennett, W.L. 2003. The burglar alarm that just keeps ringing: A response to Zaller. *Political Communication* 20 (2): 131–138. doi:[10.1080/10584600390211145](https://doi.org/10.1080/10584600390211145).
- Berrebi, C. 2009. The economics of terrorism and counterterrorism: What matters and is rational-choice theory helpful? In *Social science for counterterrorism: putting the pieces together*, ed. P. Davis, and K. Cragin, 151–208. Santa Monica: RAND.
- Bowers, K.J., and S.D. Johnson. 2003. Measuring the geographical displacement and diffusion of benefit effects of crime prevention activity. *Journal of Quantitative Criminology* 19 (3): 275–301.
- Braga, A., A. Papachristos, and D. Hureau. 2012. Hot spots policing effects on crime. *Campbell Systematic Reviews* 2012: 8. doi:[10.4073/csr.2012.8](https://doi.org/10.4073/csr.2012.8).
- Brantingham, P.L., and P.J. Brantingham. 1993. Nodes, paths, and edges: Considerations on the complexity of crime and the physical environment. *Journal of Environmental Psychology* 13 (1): 3–28.
- Cauley, J., and E. Im. 1988. Intervention policy analysis of skyjackings and other terrorist incidents. *The American Economic Review* 78 (2): 27–31.
- Clarke, R. 1980. Situational crime prevention: Theory and practice. *British Journal of Criminology* 20 (2): 136–147.
- Clarke, R. 1992. *Situational crime prevention: Successful case studies*. New York: Harrow and Heston.
- Clarke, R. 1997. Introduction. In *Situational crime prevention: Successful case studies*, 2nd ed, ed. R.V. Clarke, 1–43. Harrow and Heston: Albany.
- Clarke, R.V., and M. Felson (eds.). 1993. *Routine activity and rational choice. advances in criminological theory*, vol. 5. New Brunswick: Transaction Books.
- Clarke, R.V., and G. McGrath. 1990. Cash reduction and robbery prevention in Australian betting shops. *Security Journal* 1: 160–163.
- Clarke, R., and G. Newman. 2006. *Outsmarting the terrorists*. Westport: Praeger Security International.
- Cohen, L., and M. Felson. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44 (4): 588–608.
- Cornish, D.B., and R.V. Clarke. 1986. *Reasoning criminal: Rational choice perspectives on offending*. Secaucus: Springer.



- Cornish, D., and R. Clarke. 1987. Understanding crime displacement: An application of rational choice theory. In *The criminology theory reader*, ed. S. Henry, and W. Einstader, 45–56. New York: New York University Press.
- Cornish, D., and R. Clarke. 2003. Opportunities, precipitators, and criminal decisions: A reply to Wortley's critique of situational crime prevention. In *Theory for situational crime prevention. Crime prevention studies*, vol. 16, ed. M. Smith, and D. Cornish, 41–96. Monsey: Criminal Justice Press.
- Cozens, P.M., G. Saville, and B. Hillier. 2005. Crime prevention through environmental design (CPTED): A review and modern bibliography. *Journal of Property Management* 23 (5): 328–356.
- Crenshaw, M. 1990. The logic of terrorism: Terrorist behavior as a product of strategic choice. In *Origins of terrorism: Psychologies, ideologies, theologies, states of mind*, ed. W. Reich. Washington: Woodrow Wilson International Center for Scholars.
- Crow, W.J., and J.L. Bull. 1975. *Robbery deterrence: An applied behavior science demonstration—Final report*. Rockville: National Institute of Justice.
- Crow, W.J., and R.J. Erickson. 1984. *Cameras and silent alarms: A study of their effectiveness as a robbery deterrent*. Winslow: Athena Research Corporation.
- DiLonardo, R.L. 1996. Defining and measuring the economic benefit of electronic article surveillance. *Security Journal* 7: 3–9.
- Dugan, L., G. LaFree, and A. Piquero. 2005. Testing a rational choice model of airline hijackings. *Criminology* 43 (4): 1031–1066.
- Eck, J. 1997. Preventing crime at places. In *Preventing crime: What works, what doesn't, what's promising*, ed. L.W. Sherman, D. Gottfredson, D. MacKenzie, J. Eck, P. Reuter, and S. Bushway. Washington: U.S. Department of Justice, National Institute of Justice.
- Eck, J.E. 2002. Preventing crime at places. In *Evidence-based crime prevention*, ed. L.W. Sherman, D. Farrington, B. Welsh, and D.L. MacKenzie. New York, NY: Routledge.
- Eck, J.E., and R.T. Guerette. 2012. Place-based crime prevention: Theory, evidence, and policy. In *Oxford handbook on crime prevention*, ed. B. Welsh, and D.P. Farrington, 354–383. New York: Oxford University Press.
- Eck, J.E., R.V. Clarke, and R.T. Guerette. 2007. Risky facilities: Crime concentration in homogeneous sets of establishments and facilities. *Crime Prevention Studies* 21: 225–264.
- Eklblom, P. 1987. *Preventing robberies at sub-post offices: An evaluation of a security initiative. Crime Prevention Unit Paper No. 9*. London: Home Office.
- Eklblom, P. 1988. Preventing post office robberies in London: Effects and side effects. *Journal of Security Administration* 11: 36–43.
- Enders, W., and T. Sandler. 1993. The effectiveness of antiterrorism policies: A vector auto regression-intervention analysis. *The American Political Science Review* 87 (4): 829–844.
- Enders, W., and T. Sandler. 2000. Is transnational terrorism becoming more threatening? *Journal of Conflict Resolution* 44: 307–332.
- Enders, W., T. Sandler, and J. Cauley. 1990. UN conventions, terrorism, and retaliation in the fight against terrorism: An econometric evaluation. *Terrorism and Political Violence* 2 (1): 83.
- Farrington, D.P., S. Bowen, A. Buckle, T. Burns-Howell, J. Burrows, and M. Speed. 1993. An experiment on the prevention of shoplifting. In *Crime prevention studies*, vol. 1, ed. R.V. Clarke, 93–119. Monsey: Criminal Justice Press.
- Felson, M. 1994. *Crime and everyday life: Insight and implications for society*. Thousand Oaks: Pine Forge Press.
- Felson, M., R. Berends, B. Richardson, and A. Veno. 1997. Reducing pub hopping and related crime. In *Crime prevention studies*, vol. 7, ed. R. Homel, 115–132. Monsey: Criminal Justice Press.
- Gibbs, J. 1968. Crime, punishment, and deterrence. *Southwestern Social Science Quarterly* 48: 515–530.
- Gill, C., Lum, C., Cave, B., Dario, L., Telep C., Vitter Z., and Weisburd, D. 2012. *Evidence-based assessment of the City of Seattle's crime prevention programs*. Seattle: City of Seattle Office of City Auditor. <http://www.seattle.gov/audit/2012.htm#crimeprevention>.
- Goldstein, H. 1990. *Problem-oriented policing*. New York: McGraw Hill.
- Government Accountability Office. 2010 Testimony before the Subcommittee on Federal Workforce, Postal Service and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives: Ongoing Challenges Impact the Federal Protective Service's Ability to Protect Federal Facilities (GAO-10-506T). Washington: Government Accountability Office. <http://www.gao.gov/products/GAO-10-506T>.
- Government Accountability Office. 2012a Report to the Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of



- Representatives: Actions Needed to Assess risk and Better Manage Contract Guards at Federal Facilities (GAO-12-739). Washington: U.S. Government Accountability Office. <http://www.gao.gov/assets/600/593509.pdf>.
- Government Accountability Office. 2012b Report to the Ranking Member, Committee on Homeland Security, House of Representatives: Better Data on Facility Jurisdictions Needed to Enhance Collaboration with State and Local Law Enforcement (GAO-12-434). Washington: Government Accountability Office. <http://www.gao.gov/assets/590/589628.pdf>.
- Griffiths, M. 2003. *Town centre CCTV: An examination of crime reduction in Gillingham, Kent*. Kent: University of Reading.
- Guerette, R.T., and K.J. Bowers. 2009. Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology* 47 (4): 1331–1368.
- Hannan, T.H. 1982. Bank robberies and bank security precautions. *Journal of Legal Studies* 11: 83–92.
- Hesseling, R. 1995. Theft from cars: Reduced or displaced? *European Journal of Criminal Policy and Research* 3: 79–92.
- Homel, R., M. Hauritz, R. Wortley, G. McIlwain, and R. Carvolth. 1997. Preventing alcohol-related crime through community action: The Surfers Paradise safety action project. In *Crime prevention studies*, vol. 7, ed. R.V. Clarke, 35–90. Monsey: Criminal Justice Press.
- Interagency Security Committee. 2008. *Facility security level determinations for federal facilities: An interagency security committee standard*. Washington: Department of Homeland Security.
- Interagency Security Committee. 2011. *Physical security criteria for federal facilities*. Washington: Department of Homeland Security.
- Interagency Security Committee. 2012. *The design-basis threat: An interagency security report*. Washington: Department of Homeland Security.
- Interagency Security Committee. 2013a. *The risk management process for federal facilities: An interagency security committee standard*. Washington: Department of Homeland Security.
- Interagency Security Committee. 2013b. *Best practices for armed security officers in federal facilities*. Washington: Department of Homeland Security.
- Istre, G.R., M. McCoy, D.K. Carlin, and J. McClain. 2002. Residential fire related deaths and injuries among children: Fireplay, smoke alarms, and prevention. *Injury Prevention* 8 (2): 128–132.
- Jeffery, C.R. 1971. *Crime prevention through environmental design*. Beverly Hills: Sage.
- Koper, C. 1995. Just enough police presence: Reducing crime and disorderly behavior by optimizing patrol time in crime hotspots. *Justice Quarterly* 12 (4): 649–672.
- Lasley, J. 1996. *Using traffic barriers to 'design out' crime: A program evaluation of LAPD's operation Cul-De-Sac. Report to the National Institute of Justice*. Fullerton: California State University.
- Laycock, G., and C. Austin. 1992. Crime prevention in parking facilities. *Security Journal* 3: 154–160.
- LeBeau, J.L., and K.L. Vincent. 1997. Mapping it out: Repeat-address burglary alarms and burglaries. In *Crime mapping and crime prevention*, ed. D. Weisburd, and J.T. McEwen, 289–310. Monsey: Criminal Justice Press.
- Lum, C. 2009. *Translating police research into practice. Ideas in American Policing*. Washington: Police Foundation.
- Lum, C., and L. Kennedy. 2011. Evidence-based counterterrorism policy. In *Evidence-based counterterrorism policy*, ed. C. Lum, and L. Kennedy, 3–8. New York: Springer.
- Lum, C., and C. Koper. 2011. Is crime prevention relevant to counter-terrorism? In *Criminologists on terrorism and homeland security*, ed. B. Forrest, J. Greene, and J. Lynch. Cambridge: Cambridge University Press.
- Lum, C., and C. Koper. 2014. Evidence-based policing. In *Critical issues in policing*, 7th ed, ed. R. Dunham, and G. Alpert. Long Grove: Waveland Press.
- Lum, C., and C.S. Koper. 2017. *Evidence-based policing: Translating research into practice*. Oxford: Oxford University Press.
- Lum, C., L. Kennedy, and A. Sherley. 2006. Are counter-terrorism strategies effective? The results of the Campbell Systematic Review on counter-terrorism evaluation research. *Journal of Experimental Criminology* 2 (4): 489–516.
- Lum, C., C. Koper, and C. Telep. 2011a. The evidence-based policing matrix. *Journal of Experimental Criminology* 7 (1): 3–26.
- Lum, C., C. Gill, B. Cave, J. Hibdon, and D. Weisburd. 2011b. Translational criminology: Using existing evidence for assessing TSA's comprehensive security strategy at U.S. airports. In *Evidence-based counterterrorism policy*, ed. C. Lum, and L. Kennedy, 209–251. New York: Springer.



- Lum, C., C. Telep, C.S. Koper, and J. Grieco. 2012. Receptivity to research in policing. *Justice Research and Policy* 14 (1): 61–95.
- Lum, C., P.Z. Crafton, R. Parsons, D. Beech, T. Smarr, and M. Connors. 2015. Discretion and fairness in airport security screening. *Security Journal* 28 (4): 352–373.
- Masuda, B. 1993. Credit card fraud prevention: A successful retail strategy. In *Crime prevention studies*, vol. 1, ed. R.V. Clarke, 121–134. Monsey: Criminal Justice Press.
- Masuda, B. 1996. An alternative approach to the credit card fraud problem. *Security Journal* 7 (1): 15–21.
- Matthews, R. 1993. Kerb-crawling, prostitution and multi-agency policing. Police Research Group, Crime Prevention Unit Paper 43. London: Home Office.
- Mazerolle, L., D. Hurley, and M. Chamlin. 2002. Social behavior in public space: An analysis of behavioral adaptations to CCTV. *Security Journal* 15 (3): 59–75.
- Nagin, D.S. 1998. Criminal deterrence: Research at the outset of the twenty-first century. *Crime and Justice: A Review of Research* 23: 1–42.
- Nagin, D.S. 2013. Deterrence in the twenty-first century. *Crime and Justice: A Review of Research* 42: 199–263.
- Nagin, D.S., R. Solow, and C. Lum. 2015. Deterrence, criminal opportunities and the police. *Criminology* 53 (1): 74–100.
- National Association of Convenience Stores. 1991. *Convenience store security report and recommendations: November 1991*. Alexandria: National Association of Convenience Stores.
- National Research Council, The National Academies. 2004. *Fairness and effectiveness in policing*. Washington: National Academies Press.
- Newman, O. 1996. *Creating defensible space*. Washington: U.S. Department of Housing and Urban Development.
- Painter, K., and D.P. Farrington. 1997. The crime-reducing effect of improved street lighting: The Dudley Project. In *Situational crime prevention: Successful case studies*, 2nd ed, ed. R.V. Clarke, 209–226. Harrow and Heston: Gilderland.
- Painter, K., and D.P. Farrington. 1999a. Improved street lighting: Crime-reducing effects and cost–benefit analyses. *Security Journal* 12: 17–32.
- Painter, K., and D.P. Farrington. 1999b. Street lighting and crime: Diffusion of benefits in the Stoke-on-Trent Project. *Crime Prevention Studies* 10: 77–122.
- Painter, K., and D. Farrington. 2001. Evaluating situational crime prevention using a young person’s survey. *British Journal of Criminology* 41: 266–284.
- Popkin, S.J., V.E. Gwiasda, D.P. Rosenbaum, A.A. Anderson, L.M. Olson, A.J. Lurigio, and N. Taluc. 1995. *An evaluation of the Chicago housing authority’s anti-drug initiative: A model of comprehensive crime prevention in public housing*. Cambridge: Abt Associates.
- Poyner, B. 1991. Situational crime prevention in two parking facilities. *Security Journal* 2: 96–101.
- Poyner, B. 1994. Lessons from Lisson Green: An evaluation of walkway demolition on a British housing estate. In *Crime prevention studies*, vol. 3, ed. R. Clarke, 127–150. Monsey: Criminal Justice Press.
- Putnam, S.L., I.R. Rockett, and M.K. Campbell. 1993. Methodological issues in community-based alcohol-related injury prevention projects: Attribution of program effects. In *Experience with community action projects: New research in the prevention of alcohol and other drug problems*, ed. T.K. Greenfield, and R. Zimmerman. Rockville: U.S. Department of Health and Human Services.
- Ratcliffe, J.H., and T. Taniguchi. 2008. Is crime higher around drug-gang street corners? Two spatial approaches to the relationship between gang set spaces and local crime levels. *Crime Patterns and Analysis* 1 (1): 23–46.
- Reese, S., and L. Tong. 2010. *Federal building and facility security*, R41138. Washington: Congressional Research Service.
- Roncek, D.W. 1981. Dangerous places: Crime and the residential environment. *Social Forces* 60 (1): 74–96.
- Rothstein, H. 2007. Publication bias as a threat to the validity of meta-analytic results. *Journal of Experimental Criminology* 4 (1): 61–81.
- Runyan, C.W., R.C. Zakocs, and C. Zwerling. 2000. Administrative and behavioral interventions for workplace violence prevention. *American Journal of Preventative Medicine* 18: 116–127.
- Saltz, R.F. 1987. The role of bars and restaurants in preventing alcohol-impaired driving: An evaluation of server education. *Evaluation in Health Professions* 10: 5–27.
- Sampson, R. 2011 *False burglar alarm*, 2nd ed. Washington: U.S. Office of Community Oriented Policing Services. Problem Oriented Guides for Police: Problem Specific Guides Series, Guide No. 5.



- Sarno, C., M. Hough, and M. Bulos. 1999. *Developing a picture of CCTV in Southwark Town Centres. Final report*. London: South Bank University.
- Sherman, L. 1990. Police crackdowns: Initial and residual deterrence. *Crime and Justice: An Annual Review of Research* 12: 1–48.
- Sherman, L. 1998. *Evidence-based policing*. Washington: Police Foundation.
- Sherman, L., and J. Eck. 2002. Policing for crime prevention. In *Evidence-based crime prevention*, ed. L. Sherman, D. Farrington, B. Welsh, and D. MacKenzie, 295–329. New York: Routledge.
- Sherman, L.W., and D. Weisburd. 1995. General deterrent effects of police patrol in crime “hot spots”: A randomized, controlled trial. *Justice Quarterly* 12 (4): 625–648.
- Sherman, L., P. Gartin, and M. Buerger. 1989. Hot spots of predatory crime. *Criminology* 27 (1): 27–56.
- Sherman, L., J. Shaw, and D. Rogan. 1995. *The Kansas city gun experiment (research in brief)*. Washington: U.S. National Institute of Justice, Department of Justice.
- Sherman, L., D. Gottfredson, D. MacKenzie, J. Eck, P. Reuter, and S. Bushway. 1997. *Preventing crime: What works, what doesn't, what's promising*. Washington: U.S. Department of Justice. Report to the U.S. Congress.
- Simons, K.M., and D. Sutter. 2004. Improvements in tornado warnings and tornado casualties. *International Journal of Mass Emergencies and Disasters* 24: 352–369.
- Tilley, N. 1993. Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities. Crime Prevention Unit Series Paper 42. London: Home Office.
- Tilley, N. and Webb, J. 1994 Burglary Reduction: Findings from Safer Cities Schemes. Crime Prevention Unit Paper 51. London: Home Office.
- Tittle, C. 1969. Crime rates and legal sanctions. *Social Problems* 16: 409–423.
- United States Marshals Service. 1995 Vulnerability assessment of federal facilities. Washington: Department of Justice. <https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf>.
- Veigas, H., and C. Lum. 2013. Assessing the evidence base of a police service patrol portfolio. *Policing: A Journal of Policy and Practice* 7 (3): 248–262.
- Weisburd, D.L. 2002. From criminals to criminal contexts: Reorienting crime prevention. In *Crime & social organization: Advances in criminological theory*, vol. 10, ed. E. Waring, and D. Weisburd, 197–216. New Brunswick: Transactions Publishers.
- Weisburd, D., and J.E. Eck. 2004. What can police do to reduce crime, disorder, and fear? *Annals of the American Academy of Political and Social Science* 593: 42–65.
- Weisburd, D., C. Lum, and A. Petrosino. 2001. Does research design affect study outcomes in criminal justice? *The Annals of the American Academy of Political and Social Science* 578 (1): 50–70.
- Weisburd, D., S. Bushway, C. Lum, and S. Yang. 2004. Trajectories of crime at places: A longitudinal study of street segments in the city of Seattle. *Criminology* 42 (2): 283–321.
- Weisburd, D., L. Wyckoff, J. Ready, J. Eck, J.C. Hinkle, and F. Gajewski. 2006. Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology* 44 (3): 549–591.
- Weisburd, D., C.W. Telep, J. Hinkle, and J.E. Eck. 2010. Is problem-oriented policing effective in reducing crime and disorder? *Criminology and Public Policy* 9 (1): 139–172.
- Weisburd, D., E. Groff, and S.M. Yang. 2012. *The criminology of place: Street segments and our understanding of the crime problem*. Oxford: Oxford University Press.
- Welsh, B., and D. Farrington. 2008a. Effects of closed circuit television surveillance on crime. *Campbell Systematic Reviews* 2008: 17. doi:10.4073/csr.2008.17.
- Welsh, B., and D. Farrington. 2008b. Effects of improved street lighting on crime. *Campbell Systematic Reviews* 2008: 13. doi:10.4073/csr.2008.13.

