Making a Business Case for Security

An Interagency Security Committee Best Practice

2023 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Message from the Interagency Security Committee Chief

The Interagency Security Committee (ISC) vision statement is: "*Federal facilities, the people who work at them, and those who visit them are safe and secure throughout the country*." The ISC achieves its vision by establishing security policies, ensuring compliance, and enhancing the quality and effectiveness of security and protection of federal facilities. Chaired by the Cybersecurity and Infrastructure Security Agency's (CISA) Executive Assistant Director for Infrastructure Security, the ISC consists of 66 departments and agencies working collaboratively to achieve its vision.

As Chief of the ISC, I am pleased to introduce *Making a Business Case for Security: An Interagency Security Committee Best Practice, 2022 Edition*. Increasingly complex security challenges and a dynamic threat environment necessitate the requirement for a strong and agile security planning, programming and budgeting process. To that end, this publication assists security professionals in constructing a decision-making process or rationale for proceeding with a security project or security program, completing a benefit-cost analysis (BCA) to support spending decisions, applying these concepts to the ISC Risk Management Process, and measuring success.

This best practice guide represents exemplary leadership from the Making a Business Case for Security Working Group and collaboration across the entire ISC membership.

Daryle J. Hernandez
Chief, Interagency Security Committee
Cybersecurity and Infrastructure Agency
Department of Homeland Security

Table of Contents

Message from the Interagency Security Committee Chief **2**
Table of Contents **3**
1.0 Introduction **4**
2.0 Background **4**
3.0 Applicability and Scope **4**
4.0 Key Definitions **5**
5.0 Making a Business Case for Security **6**
5.1 How to Build a Case for Security **6**
5.1.1 Establish a Security Project Team 7
5.1.2 Conduct a Risk Assessment 7
5.1.3 Develop a Benefit-Cost Analysis 7
5.1.4 Anticipate Potential Resistance Factors 8
5.1.5 Develop Implementation Plan, Schedule, and Performance Criteria 8
5.1.6 Develop and Deliver Recommendation 8
5.2 Project Management **9**
6.0 Developing a Benefit-Cost Analysis (BCA) **10**
6.1 OMB Methodology **10**
6.1.1 OMB Circular A-4 10
6.1.2 OMB Circular A-94 11
6.2 OMB Nine Step Benefit-Cost Methodology **11**
6.2.1 Describe the Need 13
6.2.2 Define the Baseline 14
6.2.3 Set the Time Horizon for the Analysis 15
6.2.4 Identify a Range of Alternatives 16
6.2.5 Identify the Consequences of Alternatives 17
6.2.6 Quantify and Monetize the Benefits and Costs 18
6.2.7 Discount Future Costs and Benefits (Optional Step) 22
6.2.8 Evaluate Non-Quantified and Non-Monetized Benefits and Costs 23
6.2.9 Characterize Uncertainty in Benefits, Costs, and Net Benefits 26
6.3 U.S. Army Cost Benefit Analysis Guide **26**
7.0 Selecting Cost-Effective or Alternative Solutions **28**
8.0 Application within the Risk Management Process **28**
8.1 Risk Assessments **29**
9.0 Measuring Success **30**
9.1 Performance Measures **30**
Appendix A: Factors for Identifying Alternatives **32**
Appendix B: Labor Rate Calculation **37**
Appendix C: Additional Details to Quantify and Monetize the Benefits and Costs **38**
Appendix D: Discounting **40**
Appendix E: Resources **41**
E.1: Acronyms **41**
E.2: Glossary **43**
E.3: References Cited **48**
E.4: Additional Resources **50**
Acknowledgments **51**

1.0 Introduction

Leaders can build and sustain a culture of readiness within their organizations by investing in effective budget-conscious security measures Developing the business case for security provides value to an organization by reinforcing the importance of security investments.

This best practice guide provides insight for making a business case for security, completing a benefit-cost analysis (BCA), applying these concepts to the ISC Risk Management Process, and measuring success.

2.0 Background

On April 19, 1995, at 9:02 a.m., a major explosion occurred in Oklahoma City. The source of the blast was a truck packed with explosives parked outside of the Alfred P. Murrah Federal Building. The blast destroyed the facility, which housed 14 federal agencies and The America's Kids Daycare Center. This tragedy remains the worst domestic-based terrorist attack against the United States government in our history: 168 lives were lost, including 19 children, and more than 800 people were injured.

As a result, on October 19, 1995, the president signed Executive Order (EO) 12977 establishing the "Interagency Security Committee" (ISC). EO 12977 mandates the ISC enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities, and to provide a permanent body to address continuing government-wide security for federal facilities. Since its inception, the ISC has developed and published over 20 policies, standards, and recommendations to identify, assess, and prioritize risks at federal facilities.

The ISC membership requested the development of *Making a Business Case for Security, An Interagency Security Committee Best Practice* to assist organizations in developing and presenting a business case to support security projects and programs necessary to reduce risk to federal facilities and enhance compliance with ISC standards.

3.0 Applicability and Scope

Consistent with EO 12977, *Making a Business Case for Security, An Interagency Security Committee Best Practice, 2022 Edition,* is a resource intended to assist security professionals in developing security projects or programs that enhance the security and protection of federal buildings and facilities. It is applicable to all executive branch buildings and facilities in the United States occupied by federal personnel for non-military activities. These facilities include currently owned, to be purchased, or leased facilities; standalone facilities; federal campuses; and, where appropriate, individual facilities on federal campuses and special-use facilities.

Title 41, Code of Federal Regulations (CFR), Part 102-81, *Physical Security* further specifies ISC policies and recommendations "govern physical security at Federal facilities and on Federal grounds occupied by Federal employees for nonmilitary activities." This regulation is applicable to "federally owned and leased facilities and grounds under the jurisdiction, custody, or control of GSA, including those facilities and grounds that have been delegated by the Administrator of General Services."

4.0 Key Definitions

ANNOTATED SOURCES:

1- **A4/Primer**: Office of Information and Regulatory Affairs Regulatory Impact Analysis
2- **Circular NO. A-94**: OFFICE OF MANAGEMENT AND BUDGET REGULATORY ANALYSIS
3- **Army CBA**: Office of the Deputy Assistant Secretary of the Army (Cost and Economics)
4- **DHS Lexicon**: Instruction Manual 262-12-001-01 Terms and Definitions

Key definitions below are taken from the following sources:

TERM	DEFINITION
Benefit-Cost Analysis[2]	A systematic quantitative method of assessing the desirability of government projects or policies when it is important to take a long view of future effects and a broad view of possible side-effects.
Break-Even/ Threshold Analysis[4]	Variant of cost-benefit analysis that estimates the threshold value for an uncertain parameter equating costs and benefits.
Business Case for Security	A decision-making process or rationale for proceeding with a security project or security program.
Life-Cycle Cost Estimate (LCCE)[3]	The estimated cost of developing, producing, deploying, maintaining, operating, and disposing of a system over its entire lifespan.
Non-quantifiable Benefits[1]	A benefit not lending itself to numeric valuation, such as better quality of services.
Quantifiable Benefit[3]	A benefit assigned a numeric value, such as dollars, physical count of items, or percentage change.

5.0 Making a Business Case for Security

A business case is a decision-making process or rationale for proceeding with a project or program. The business case evaluates and weighs benefits, costs, and risks of a preferred solution against alternative options to solve an identified problem or gap. The complexity of the problem or opportunity may drive the depth of the decision-making process. Though the cost of remediating a security incident is quantifiable, recovering damaged infrastructure and reputation can be difficult to assess. The cost to recover from a security incident may be more expensive than the cost of preventing such events. Further, reputational damage can be difficult to fully repair.

In 2016, a large beverage company announced that an unspecified number of laptops had been stolen and information on 74,000 current and former employees may have been compromised.

5.1 How to Build a Case for Security

Security professionals can tailor their business case to present a specific security investment or to propose a broader initiative, such as converged or integrated cybersecurity and physical security functions. Regardless of the security investment, the process and business case components remain the same and should contain the general elements found in Figure 1**. Each element is further described in sections 5.1.1 – 5.1.6.**

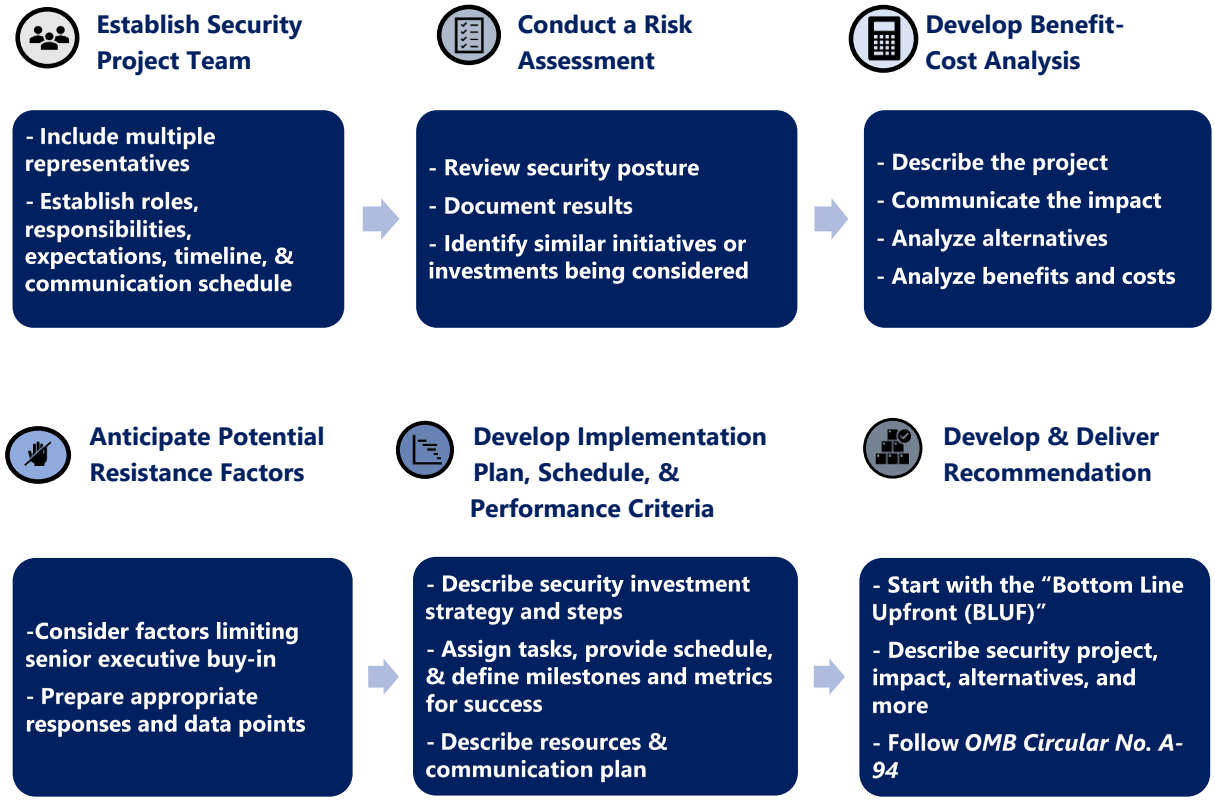


Figure 1: Elements for Creating a Business Case for Security At-a-Glance

5.1.1 Establish a Security Project Team

Selecting the right team is a critical first step in building a successful business case and should be tailored to match the scope of the project. Examples of security project team members include representatives from the organization's physical security, information technology (IT), emergency management, facilities, finance/budget, human resources, legal, program management responsible for the mission essential function (MEF), and business continuity functional areas. The team should consider creating a charter endorsed by leadership to establish clear roles, responsibilities, expectations for involvement, a project timeline, and the team's communication schedule.

5.1.2 Conduct a Risk Assessment

Review your organization's current security posture and conduct a risk assessment to understand the organizational risks (threats, vulnerabilities, and consequences). Thoroughly document the assessment results to help define the business case rationale and identify all assets needing protection and the associated risks for each. Although assets will vary by organization, examples include classified and sensitive information and their associated spaces/servers, employees, continuity of operations, stakeholders, and facilities. For security projects related to federal facilities, organizations may be able to refer to their most recent risk assessment, which is an ISC requirement.

The ability to prioritize these risks, identify those risks that are relatively higher, and to be able to communicate the lowering of risk as a result of the security recommendation is critical to making the business case for security.

Opportunities to address security and sustainability in the same project may arise providing a greater overall return on investment (ROI). The project team should contact the organizational capital investment committee or a comparable organizational structure in charge of project planning and prioritizing as part of the risk assessment process to determine if similar initiatives or investments are being considered. When security, safety, and sustainability issues are addressed simultaneously while sharing the costs, as may be the case with glass structures (interior and exterior), both projects can save money while still achieving their individual goals and objectives.

5.1.3 Develop a Benefit-Cost Analysis

Once the risk assessment is complete, the project team develops a BCA using one of the several methodologies available. Section 6.0 details how to use the Office of Management and Budget (OMB) methodology. and Sections 5.1.3.1 – 5.1.3.4 are key sub-tasks of developing a BCA.

5.1.3.1 Describe Security Project

Using the risk assessment results, the team develops a description for the security project or program. This description is a high-level overview explaining how the intended security solution will address one or more of the risks identified in the risk assessment (Sections 6.2.1, 6.2.3).

5.1.3.2 Communicate the Business Impact

To develop this section, ensure the project documentation identifies the mission critical assets needing protection and quantifies the potential negative impacts of failing to adequately protect those assets against identified threats (see Design-Basis Threat Report[1]). First, leverage the risk assessment results, any

[1] The Risk Management Process for Federal Facilities: An ISC Standard, Appendix A: Design-Basis Threat Report, ISC Policies Standards Best Practices Guidance Documents and White Papers | CISA

available supporting data, and a prioritized list of recommendations based on highest risk and impact (Sections 5.1.2, 6.2.2, 6.2.5). Next, calculate the benefits of the recommended security investment and identify how it will positively impact the organization.

5.1.3.3 Analyze Alternatives

Analyzing alternative security investments and the potential cost of avoiding security investments will support your business case for security. An evaluation of other federal or private sector security practices will help shape options and mitigation strategies. Project teams should consider two to three tangible options addressing the identified security needs and include options with higher and lower costs, shorter or longer timeframes, and other possible variables impacting costs and benefits (Section 6.2.4).

5.1.3.4 Analyze Benefits and Costs

Effective communication of the costs and benefits of security options includes an analysis and determination of which security investments to pursue. Section 6.2 describes the analytical approaches in the evaluation of cost and benefit and includes the BCA and threshold or break-even analysis (Sections 6.2.6-6.2.9).

5.1.4 Anticipate Potential Resistance Factors

Anticipating objections to a security investment will help in preparing the necessary information and approach required to address them. Without motivating events, leaders may be hesitant to invest in preemptive and preventive security measures. While reasons often vary by an organization's size, type, location, and mission, several common objections include cost, inconvenience, distrust in security technologies, and difficulty quantifying ROI. To effectively convey the need to invest in security and the significant risks associated with inaction, the project team must consider the resistance factors affecting senior executive buy-in. Having appropriate responses and supporting data will facilitate a more favorable outcome

5.1.5 Develop Implementation Plan, Schedule, and Performance Criteria

An implementation plan describes how an organization will execute the security investment strategy and breaks down the strategy into identifiable steps; assigns tasks to personnel; provides a project schedule; and defines milestones and metrics for success. The plan should include a detailed description of the resources needed as well as a communication plan for how the roll out will impact employees and stakeholders.

5.1.6 Develop and Deliver Recommendation

In this final step, research, analysis, and recommendations transform into a presentable business case. Using the organization's preferred presentation format, the business case for security should start with the "Bottom Line Upfront (BLUF)", to orient the decision maker on the key information they are expected to decide on and follow with the security project description; business impact; analysis of alternatives; costs and benefits; implementation plan and schedule; and recommendation. The presentation should also include visuals (data, charts, or graphs) and sufficient detailed information (in reserve) to limit the need for follow-up or follow-on requests for information.

Regardless of how an organization determines to document and present their work, they should follow the four characteristics put forth in *OMB Circular No. A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs,* including a "reliable cost estimate that is well documented, comprehensive, accurate, and credible." Further, the Department of Defense (DOD) provides a sample documentation template, *DOD Business Case Analysis Template*.

5.2 Project Management

While project management is crucial to the outcome of security upgrades such as application of security countermeasures to a major modernization of a federal facility, it is beyond the scope of this document to provide detailed project management practices. Security project teams are encouraged to become familiar with and use project management methodologies. Additional information about project management can be found in the following sources:

- Federal Acquisition Institute
- Defense Acquisition University
- Graduate School USA
- Project Management Body of Knowledge (PMBOK Guide)

6.0 Developing a Benefit-Cost Analysis (BCA)

In today's environment, security organizations must compete for and manage resources. As noted in the Government Accountability Office's (GAO) GAO-15-444 *Action Needed to Better Assess Cost Effectiveness of Security Enhancements at Federal Facilities*, "Given that it is not fully known how much entities expend on enhancements and that cost factors vary by facility, it becomes an even more essential key practice that entities at both the headquarters and facility levels have the tools necessary to make sound resource allocation decisions." Developing a BCA is useful in assisting organizations as they seek funding for security countermeasures, develop essential security programs, achieve necessary staffing levels, training, and develop annual budget submissions.

6.1 OMB Methodology

Executive Order (EO) 12866 – *Regulatory Planning and Review*[2] requires agencies to conduct a regulatory analysis for economically significant regulatory actions.[3] EO 13563 – *Improving Regulation and Regulatory Review* also requires agencies to use the best available techniques to quantify anticipated present and future benefits and costs as accurately as possible for economically significant actions.[4] OMB Circular[5] A-4 assists federal agencies in developing regulatory analysis by standardizing the way benefits and costs of federal regulatory actions are measured and reported while Circular A-94 supports the processes outlined in it.

Although OMB's methodology is primarily for regulatory analysis, its model can inform a best practice in justifying security needs to organizational leadership and financial offices through effective documentation, analysis, and a presentation framework.

Following and relating the practices within OMB Circulars A-4 and A-94 to a security project assists organizations in creating a common language between the office justifying the security need and the financial office analyzing its financial viability.

6.1.1 OMB Circular A-4

Implementing a regulatory impact analysis (RIA) as described in OMB Circular A-4 ensures consideration of consequences prior to taking regulatory action. The benefits and costs projected to result from the proposed action and anticipated regulatory measures are evaluated, quantified, and, to the extent practical, valued in this analysis. The RIA process also considers the effects of abstract elements like policy and economic impacts.

---

[2] Executive Order 12866 was issued in 1993. It provides significant regulatory actions be submitted for review to the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB).

[3] Executive Order 12866 refers to "those matters identified as, or determined by the Administrator of OIRA to be, a significant regulatory action within the scope of section 3(f)(1)."

[4] Executive Order 13563 sets out "principles and requirements designed to promote public participation, improve integration and innovation, increase flexibility, ensure scientific integrity, and increase retrospective analysis of existing rules."

[5] The Office of Management and Budget (OMB) prescribes circulars and bulletins as major tools used by the Executive Office of the President to exercise managerial and policy direction over federal agencies.

6.1.2 OMB Circular A-94

OMB Circular No. A-94 , a companion document to the A-4, provides a more in-depth explanation of the processes identified in the base document and serves as a checklist for considering and properly dealing with all analytical elements, including:

- Efficient resource allocation through well-informed decision-making
- General guidance for conducting BCAs and cost-effectiveness analyses
- Specific guidance on discount rates to be used in evaluating federal programs when benefits and costs are distributed over time
- Guidance for any analysis used to support government decisions to initiate, renew, or expand programs or projects resulting in measurable benefits or costs extending three or more years into the future

6.2 OMB Nine Step Benefit-Cost Methodology

OMB Circular A-4 outlines nine steps in preparing a regulatory impact analysis for agency rulemaking.[6] This document demonstrates how an organization may adapt OMB's nine steps in developing a BCA to provide a thorough analysis for decision makers to consider.

[6] Rulemaking is the policy-making process for executive and independent agencies of the federal government to develop and issue rules, also referred to as "regulations". The process is governed by laws such as the Administrative Procedure Act (APA), Congressional Review Act, Paperwork Reduction Act, and Regulatory Flexibility Act. Executive orders such as 12866, 13563, and 13579 also establish principles and guidance for the rulemaking process. To learn more about rulemaking visit: https://www.regulations.gov/learn.

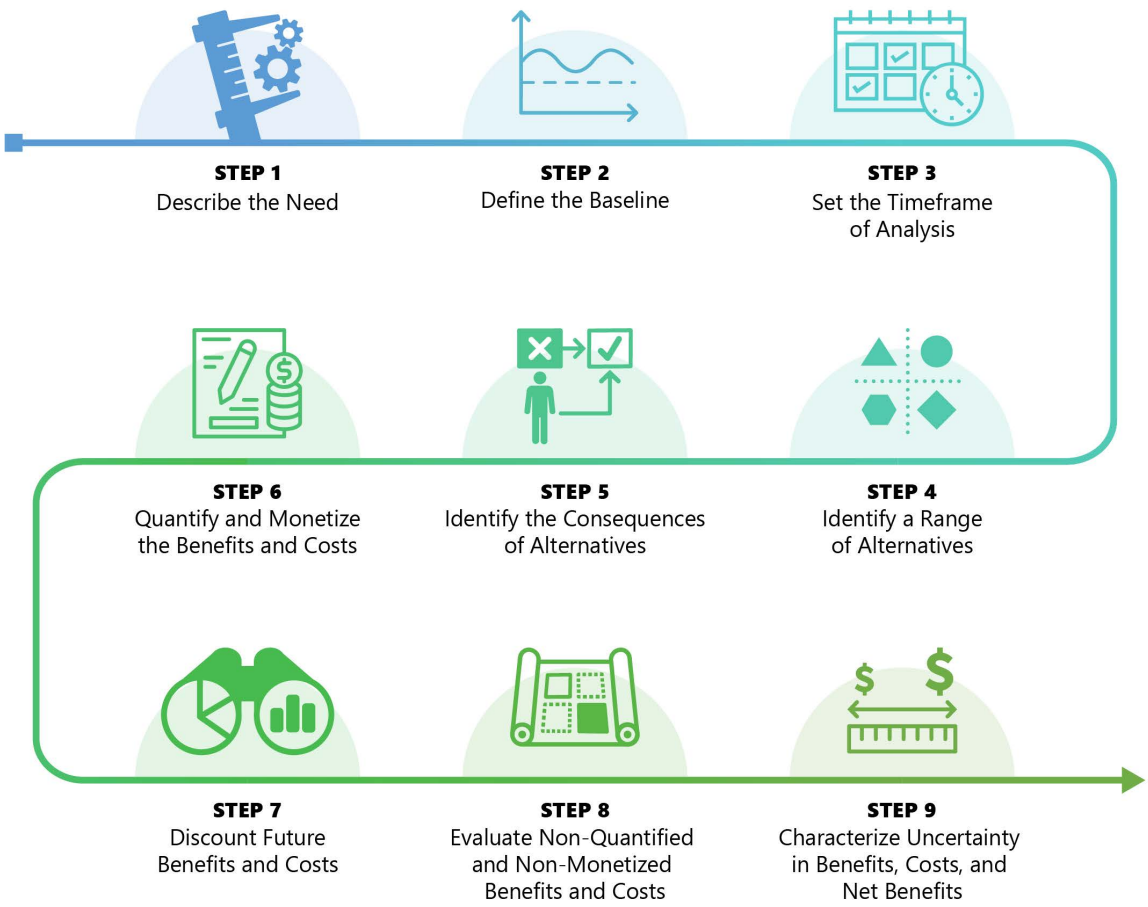


Figure 2: OMB Nine Step BCA Methodology

A hypothetical case study scenario in Figure 3 provides an example of each step. A **blue border** denotes a case study example.

CASE STUDY SCENARIO

A single-tenant, federal facility has a current risk assessment identifying multiple risks associated with the main entrance and screening area. The facility is in a metropolitan area and processes several hundred visitors daily. In the past 24 months, the facility has been the scene of several protests, and on two separate occasions, the facility security force detected attempts to enter the facility by non-employees utilizing counterfeit credentials.

As a result of fiscal constraints and competing priorities, the federal tenant has been accepting the associated risk identified in the assessment. Recently, the state government has relocated several offices into an adjacent facility. The state office staff has received numerous credible threats including threats of violence directed at the office staff. The entrances to the federal and state facilities look similar and there have been several occurrences where visitors attempted to enter the federal facility believing it housed state offices. One incident resulted in verbal threats toward an armed contract security officer (ACSO) necessitating local law enforcement to intervene and escort the person from the facility.

Figure 3: Case Study Scenario

6.2.1 Describe the Need

Before recommending an action, organizations must demonstrate the proposed action is necessary by creating a reasonably detailed description of what is needed and why. The goal is to explain the problem and what action is needed to resolve the problem. Sources that can be the catalyst for such actions include, but are not limited to:

- Identified vulnerability from a risk assessment
- Compliance with regulatory or executive order requirements such as Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*
- Adjusting to organizational mission changes
- Lifecycle replacement or upgrade of electronic security systems (ESS)
- Additional staffing necessary to meet mission demands
- System failure or other identified gap or vulnerability resulting from an undesirable event (UE) or other incident or as part of annual functionality testing
- Lessons learned or another risk mitigation strategy for meeting evolving threats

Development of a problem or opportunity statement clearly defining the problem and required capability can be useful when describing the need (see Figure 4).

Problem/Opportunity or "The Need": The facility received risk assessments in 2015, 2018, and 2021 as required in the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. Each risk assessment identified risks associated with the facility entrance screening area, lobby, and visitor processing area. More specifically, the following items were identified:

- A substantial number of unscreened personnel queued outside the secure area awaiting entry exposing them to a variety of risks.
- The security force lacks personal ballistic protection.
- A lack of a ballistic protective barrier in the utilization of security force booths, desks, or podiums where armed security forces and other security personnel are stationed when interacting with unscreened personnel.
- Employees and visitors share the same entrance with an intermingled flow pattern hindering the ability of the security force to conduct visual and physical inspection of employee badges before entry. Additionally, it exposes employees to unscreened visitors.
- Windows and door glass do not meet blast resistance requirements.

The combined effect is an increased risk of a variety of undesirable events such as active shooter, breach of access control point, theft, unauthorized entry, and an assortment of explosive devices as described in the ISC's *Appendix A: The Design-Basis Threat Report*.

Possible Solution: A reconfigured lobby with additional visitor screening lanes, separate visitor and employee flow-patterns, and a consolidated access control office and visitor center would significantly reduce the risk to the facility. Increased throughput for visitors not only reduces exposure from queuing outside the security screening but enhances the overall customer experience. Additionally, ballistic protection for the security force is necessary to increase response capabilities reducing the risk to the facility even further.

Figure 4: Case Study Scenario - Step One: Describe the Need

6.2.2 Define the Baseline

The primary purpose of the baseline is to provide decision makers with a picture and impact of inaction, and a secondary use of informing performance measures. The baseline represents the current state and the organization's best assessment of what the world would be like in the absence of a specific action. To specify the baseline, the organization may need to consider a wide range of factors including the organization's best forecast of how the world will change in the future.[7] For example, organizations should consider evolution of risks or future changes in mission. However, this step should not be confused with the "baseline level of protection" used in the ISC Risk Management Process.

[7] Office of Information and Regulatory Affairs "Regulatory Impact Analysis: A Primer" Published August 15, 2011, https://www.reginfo.gov/public/jsp/Utilities/circular-a-4_regulatory-impact-analysis-a-primer.pdf

The public can access the facility via the door and step into an open area with four employee turnstiles and a single visitor screening lane with one x-ray and magnetometer. There are three ACSOs supporting the screening lane. Due to a single visitor lane and large numbers of visitors, the queue for visitors often goes outside the building and wraps along the facility perimeter. A fourth ACSO is assigned to process visitors (sign-in, issue a visitor badge, and monitor until an escort arrives), provide overwatch screening operation, and monitor employee turnstiles to compare employee pictures via the system monitor when the employee uses the card reader. At present, employee card readers do not have pin pads to enable multifactor authentication. The video surveillance system (VSS) was upgraded two years ago with a digital system and currently provides necessary coverage of the entrance, lobby, and screening operation. The system has capacity to add additional cameras, if warranted.

Body armor has not been provided to the security force at the access control point and blast resistance glazing or treatment on the windows and glass doors has not been applied. As noted in the risk assessments from 2015, 2018, and 2021, the multiple risks at the entrance, lobby, and screening area increase the likelihood of several events negatively impacting the facility and operations, including:

- Mass casualty events such as active shooter
- Civil disturbance/flash mobs
- Covert breach of access points
- Theft of employee/government property

Figure 5: Case Study Scenario - Step Two: Define the Baseline

6.2.3 Set the Time Horizon for the Analysis

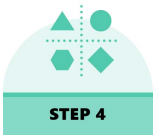
Organizations should choose an appropriate time horizon for estimating benefits and costs encompassing possible outcomes from the action. For example, the upgrade of a VSS may have a higher first year installation cost than annual repair or maintenance costs for an existing system. Yet, organizations could benefit from lower maintenance costs and increased reliability over the life span of the new system. Therefore, the analysis should cover a multi-year period to address life-cycle costs. Additionally, annual testing, benefits from the security upgrade, and maintenance costs will need consideration.

The life-cycle cost can be defined as the total cost to the government of an initiative or program over its full life, including costs for research and development, testing, production, facilities, operations, maintenance, personnel, environmental compliance, and disposal.[8] A comprehensive life-cycle cost estimate helps decisionmakers assess the long-term affordability of the initiative/program. The estimate should be analyzed and organized with respect to occurrence since some costs are non-recurring while other costs are generated each time an item is produced, or service performed.

[8] U.S. Army Cost Benefit Analysis Guide

The timeframe for the analysis has been set at 10 years based on the life-cycle of the screening equipment. [Note: Body armor would be replaced in 5 years.]

Figure 6: Case Study Scenario
Step Three: Set the Timeline Horizon for the Analysis



6.2.4 Identify a Range of Alternatives

By considering a range of potentially effective solutions or risk mitigation strategies, organizations will be able to eliminate some alternatives through preliminary analysis, leaving a manageable number of alternatives to be evaluated. The number and choice of alternatives selected for detailed analysis is a matter of judgment.

When selecting alternatives, focus should be on areas with significant impact such as comparative risk analysis[9] or major cost drivers. Appendix A provides factors, considerations, and an example scenario for organizations to use when developing alternatives, including resource solutions; vendor-oriented approaches or alternative funding options; objective-based or performance-based services; minimum standards and requirements based on size; performance monitoring; enforcement methods; stringency; implementation dates; and requirements based on geographic and other limitations.

Option 1 (preferred): The preferred solution is to reconfigure the current lobby to create three screening lanes with new screening equipment, six additional ACSOs to support visitor screening, and one additional dedicated ACSO to monitor employee access. Additionally, build out a dedicated visitor control and access control office where visitors will be signed-in and wait for escorts in a controlled area not visible to the public. Lastly, provide appropriate level of body armor for the security force in contact with the public, install three ballistic ACSO podiums, and install blast resistance technology meeting the current Design Basis Threat (DBT) to windows and glass doors.

Option 2 (minimum recommendation): Add one additional screening lane, three additional ASCOs to support visitor screening, and one additional dedicated ACSO to monitor employee access. Include body armor for the security force.

Option 3 (status quo):
Remain at current baseline and continue to accept risk (see figure 5).

Figure 7: Case Study Scenario - Step Four: Identify Alternatives

[9] When considering alternatives, it may also be useful to identify programs or facilities that may be considered mission essential and establish parameters and priorities for their protection.

6.2.5 Identify the Consequences of Alternatives

After identifying feasible and potentially effective alternatives, the next step is to identify prospective benefits and costs. It may be useful to identify costs in the following manner:

- Benefits and costs that can be monetized
- Benefits and costs that can be quantified, but not monetized
- Benefits and costs that cannot be quantified

In addition to the direct benefits and costs, identify the expected undesirable side-effects and ancillary benefits of the alternatives. For example, if the intent is to mitigate against an insider threat, but the alternative may also reduce the likelihood of success for other criminal activity, the direct benefits and costs should be added as appropriate. It is also important to note why a particular alternative was rejected as compared to the preferred alternative or proposed option.

An ancillary benefit is an unrelated positive impact of the alternative being considered, not directly connected to the designed security benefits.

Finally, organizations should note those who bear the costs of the baseline, proposed action, and alternatives and those who enjoy the benefits are often not the same. This is referred to as the "distributional effect" and describes the impact an alternative creates across the various parties. Where a distributional effect exists, it should be included in the analysis.

The goal of *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP), 2021 Edition,* (RMP) is to identify an achievable level of protection (LOP) commensurate with—or as close as possible to—the level of risk without exceeding it. The consequences and amount of risk accepted is directly proportional to the option selected.

Option 1 Consequences (Preferred)

- Reduces target attractiveness
- Reduces risk of mass casualty events such as an active shooter
- Mitigates risk identified in three risk assessments during past seven years
- Reduces queuing outside screening areas
- Reduces congestion in public access areas
- Enhances response capabilities of security force to an undesirable event
- Reduces risk of unauthorized access to facility
- Deters introduction of prohibited items such as firearms
- Enhances overall customer experience and increased efficiency of visitor throughput

Option 2 Consequences

- Enhances response capabilities of security force to an undesirable event
- Partially mitigates risk associated with long screening lines
- Tenant accepts unmitigated risk

Option 3 Consequences

- All identified risk remains unmitigated
- Tenant accepts unmitigated risk

Figure 8: Case Study Scenario- Step Five: Identify the Consequences of Alternatives

6.2.6 Quantify and Monetize the Benefits and Costs

Organizations should seek the best reasonably obtainable data to quantify the likely benefits and costs of the proposed option and each alternative. Presenting benefits and costs in physical units in addition to monetary units provides a comprehensive picture of the proposed business case. In completing the analysis, organizations should include items like administrative costs and savings or gains/losses in productivity or efficiency.

6.2.6.1 Quantifying Benefits

Quantifiable benefits are assigned a numeric value such as dollars, physical count of tangible items, or percentage change. The benefits may stem from cost reductions or savings due to changes to the baseline. The benefit of an alternative may be the reduction in likelihood of an undesirable event or the reduction in consequence from such an event. Figure 9 provides an example of quantifiable benefits based on the case study scenario.

The ISC's *Armed Contract Security Officers in Federal Facilities: An Interagency Security Committee Best Practice, Appendix C* provides factors to estimate the number of ACSOs needed to perform specific security functions for a facility. Key data points used to develop an analysis include:

- Completing the basic personnel and package screening processes (the individual successfully passes metal detector examination, and their belongings successfully pass Xray examination) typically requires 45 to 60 seconds per person.
- Wanding/secondary screening of individuals adds an additional 90 seconds per person.
- In most cases, 40 persons per hour can be expected to pass through a security station without a line of people forming. This estimate includes time for up to 25 percent of persons to require secondary screening (wanding).

Using this information, a simple table illustrates some the benefits associated with each option.

	Existing System	Option 1 (Preferred)	Option 2 (Minimum Recommendation)	Option 3 (Status Quo)
Screening Lanes	1	3	2	1
ACSOs	4	11	8	4
Customers Screened	40/hour	120/hour	80/hour	40/hour
	% Increase	**200%**	**100%**	**N/A**

Quantified benefits realized from increased screening efficiency may include:

- Fewer missed appointments as customers are screened at a faster pace.
- Increased productivity of organization staff by eliminating time gaps between appointment time and customer screening times.
- Time savings for the customer due to reduced lobby queueing.

Figure 9: Case Study Scenario - Step Six: Quantify and Monetize Benefits and Costs (Benefit Analysis)

6.2.6.2 Costs

A detailed analysis and identification of the baseline is fundamental to determining additional costs and cost savings for proposed actions and alternatives. Referring to the baseline assessment performed in Step 2 of the OMB methodology, describe what is already available, currently happening, and then quantify baseline elements. Consider costs already incurred in the baseline assessment. See Appendix C for additional details on each of the below areas:

- Costs for operations and sustainment (O&S)
- Personnel or support labor costs
- Information technology costs
- Preventative maintenance and repair
- Other reoccurring or incidental costs
- Contracting and procurement costs

Creating a work breakdown structure (WBS) [10] or other cost structure establishes the cost of each element, provides a framework, and reduces redundancy in cost estimations. Consider life-cycle costs using a resource management plan encompassing all phases of a product's useful life, from the initial planning stage to deployment to end user. Further, make sure to document ground rules and assumptions. The *ISC Making a Business Case – Cost Analysis Template*[11] was created to assist organizations in calculating costs. Figure 10 and Figure 11 correspond to the case study and represent the template format.

Figure 10 shows the associated inputs of the preferred option, (the individual components required to reconfigure the lobby, build out the access control center, and increase the number of screening lanes), their estimate costs, and assumed life-cycle. This provides a basis to begin monetizing the benefits. Figure 11 provides the total cost associated with implementing the preferred option through the time horizon of the analysis (10 years), as identified in Step 3.

Cost Analysis Inputs	**Entrance/Lobby Reconfiguration**		
Description	Estimated Cost or Input	Assumed Useful Life	Notes, assumptions
Design & Architecture	$50,000	N/A	Cost is incurred in year 0, one time cost
Installation	$100,000	N/A	Cost is in year 1, and is one time cost
Guards	$450,000	N/A	Security force (first year cost), reoccurring with % increase each year
Percentage Increase in Guard Costs	6%	N/A	Applies to each subsequent year
Visitor seats	$15,000	10	30 seats needed
Workstations	$10,000	5	Employee workstations for 8 employees
Workstations (Replacement)	$10,000	5	Replacement costs for workstations
Ballistic Guard Reception Desk	$100,000	10	Ballistic desk for security force reception employees
Ballistic Equipment	$50,000	5	Initial issue
Ballistic Equipment (Replacement)	$50,000	5	Replacement costs for ballistic equipment
X-Ray/ magnetometer	$150,000	10	One-time cost, preventative maintenance included in another category
Preventative Maintenance	$10,000	N/A	

Figure 10: Case Study Scenario - Step Six: Quantify and Monetize Benefits and Costs (Cost Analysis Inputs)

[10] For more information on WBS, see the GAO Cost Estimation and Assessment Guide. Published March 2020. https://www.gao.gov/pdf/product/705312

[11] ISC Making a Business Case – Cost Analysis Template

Preferred Option Costs by Year									
Year	Design & Architecture	Installation	Guards	Visitor seats Workstations	Ballistic Guard Reception Desk	Ballistic Equipment	X-Ray/ magneto-meter	Preventative Maintenance	Total Cost (Undiscounted)
0	$50,000	$0	$0	$0	$0	$0	$0	$0	$50,000
1	$0	$100,000	$450,000	$25,000	$100,000	$50,000	$150,000	$0	$875,000
2	$0	$0	$477,000	$0	$0	$0	$0	$10,000	$487,000
3	$0	$0	$505,620	$0	$0	$0	$0	$10,000	$515,620
4	$0	$0	$535,957	$0	$0	$0	$0	$10,000	$545,957
5	$0	$0	$568,115	$0	$0	$0	$0	$10,000	$578,115
6	$0	$0	$602,202	$10,000	$0	$50,000	$0	$10,000	$672,202
7	$0	$0	$638,334	$0	$0	$0	$0	$10,000	$648,334
8	$0	$0	$676,634	$0	$0	$0	$0	$10,000	$686,634
9	$0	$0	$717,232	$0	$0	$0	$0	$10,000	$727,232
10	$0	$0	$760,266	$0	$0	$0	$0	$10,000	$770,266
Total	**$0**	**$100,000**	**$5,931,358**	**$35,000**	**$100,000**	**$100,000**	**$150,000**	**$90,000**	**$6,556,358**
							Annual Average Cost = Total Costs ÷ 11 years =		**$596,033**

Figure 11: Case Study Scenario -Step Six: Quantify and Monetize Benefits and Costs (Preferred Option Costs by Year)

Efforts to reduce security risks may also reduce risks to life. In these instances, evaluation of the benefits of reducing fatality risks should be a key part of the analysis. Organizations may use a concept called "value of statistical life" (VSL) to quantify an individual's willingness to pay (WTP) to avoid premature death.

The goal of this type of analysis is to monetize the value of small changes in fatality risk – a measurement of WTP for reductions in only small risks of premature death. A considerable body of academic literature is available on this subject. Organizations may use a VSL of $11.6 million (2020$).[12] Notably, the VSL is not attempting to place a value on a human life but is instead attempting to value the reduction of mortality risks in the context of low probability events. **For example, a $11.6 million VSL does not mean that a specific human life is worth $11.6 million; it means this is what people are willing to pay to reduce low-level mortality risks, or what people demand to face such risks (say, $116 for a risk of 1 in 100,000).**

When estimating the value of a statistical injury, consider the US Department of Transportation (DOT) methodology[13] based on the Abbreviated Injury Scale (AIS) to calculate non-fatal injury costs as a percentage of the VSL. Table 1 provides the relative disutility factor based on the type of injury.

[12] Department of Homeland Security, *Best Practices for the Treatment of Statistical Life in U.S. Department of Homeland Security Regulatory Analyses*, April 2021. Available at: Best Practices for the Treatment of Statistical Life in U.S. Department of Homeland Security Regulatory Analyses. Department of Transportation, 2021 Guidance: Departmental Guidance on Valuation of a Statistical Life in Economic Analysis | US Department of Transportation . Additionally, if agencies prefer to use a range, Health and Human Services practices provide a VSL ranging from roughly $5.3 (2020$) million to $17.4 (2020$) million per statistical life. For more information, see U.S. Department of Health and Human Services (HHS) 2016 *Guidelines for Regulatory Impact Analysis*. Available at: Guidelines for Regulatory Impact Analysis | ASPE (hhs.gov).

[13] Adverse or harmful effects associated with a particular activity.

Table 1: Relative Disutility Factor by Injury Severity Level

AIS Code	Description of Injury	Fractional Fatality Values of VSL
AIS 1	Minor	0.003
AIS 2	Moderate	0.047
AIS 3	Serious	0.105
AIS 4	Severe	0.266
AIS 5	Critical	0.593
AIS 6	Fatal	1

To calculate the consequence of a UE where human injuries or loss of life occur, multiply the number of fatalities by the VSL of $11.6 million. Then multiply "the cost per averted injury by type of injury (AIS Code)" by the number of each type of injury. For example, using the DOT recommendation (Table 1), a disutility factor of 26.6 percent applies for severe injuries as below:

$11.6M x .266 = $3.09M
[The organization would then multiply the number of severe injuries x $3.09M.]

Under the AIS, examples of severe injuries include a spleen rupture or a chest-wall perforation while examples of a moderate injury include a major abrasion or laceration of skin.[14] Section 6.2.8 (Step 8) demonstrates how to use VSL calculations as part of a break-even analysis.

6.2.7 Discount Future Costs and Benefits (Optional Step)

Discounting allows comparison of security benefits and costs occurring in the past with possible occurrences in the future. There is an opportunity cost to spending money now but also benefits realized sooner than later. An opportunity cost means the money spent on the proposed option could be spent on something else, invested, or used to reduce debt. In most business cases, organizations will not need to discount costs and benefits. Few instances, such as business cases with over $100M in costs, should apply discounting. For more details on discounting refer to Appendix D.

[14] Sample types of injuries used by in the Abbreviated Injury Scale can be found in "Economic Values for FAA Investment and Regulatory Decisions, A Guide Final Report", page 2-2. https://www.faa.gov/regulations_policies/policy_guidance/benefit_cost/media/econ-value-section-2-txvalues.pdf, Updated September 2016.

6.2.8 Evaluate Non-Quantified and Non-Monetized Benefits and Costs

Some benefits and costs, like deterrence of a security incident or UE, do not lend themselves to direct, quantitative analysis. Deterrence is a security principle often sought by security professionals by "hardening of the target" or reducing the "target attractiveness". The ability to deter a security incident or UE from occurring is non-quantifiable because of the difficulty determining the number of attacks deterred based on the proposed security measure. Non-quantifiable benefits rely on a qualitative narrative to contribute value add to the analysis. Benefits and costs difficult to quantify and monetize may be evaluated using break-even or threshold analysis or development of a non-quantifiable table of benefits.

6.2.8.1 Break-even analysis

When it is not possible to quantify or monetize the key benefit components of a security measure, organizations may conduct a break-even (or threshold) analysis by comparing the estimated costs to implement the security measures with the estimated monetary value of avoiding a successful attack. A breakeven analysis uses evaluation of direct consequences from a UE, such as injuries; loss of life; onsite business/service interruption; immediate remediation costs; and damage to property and infrastructure as well as to the environment. For example, direct consequences of an averted or deterred security incident (or averted costs) include the monetized value of avoided fatalities, nonfatal injuries and hospitalizations, property damage, and rescue and cleanup costs. Dividing the averted costs of a security incident or UE by the annualized cost of the security measures results in the number of such incidents to be avoided on an annual basis for the benefits to equal the costs. An indirect consequence is an effect not associated with an event, incident, or occurrence, but is caused by a direct consequence, subsequent cascading effects, and/or related decisions.

When considering a security benefit analysis, it is important to tie the effectiveness of the proposed countermeasures to the security incident or UE. Therefore, organizations should consider scenarios where the security measure is reasonably expected to reduce the likelihood of the scenario. For example, if a measure is intended to prevent an insider threat, the direct consequences of an insider threat security incident should be estimated. If the measures being considered are intended to reduce risk of a cyber threat, a possible cyber breach and the direct consequences of a breach could be used in a breakeven analysis. CISA has published reports on the costs of cyber incidents that may serve as a reference for cyber cost estimates.[15] Figure 12 below provides the VSL calculation using the single undesirable event of an active shooter.

[15] Cybersecurity and Infrastructure Security Agency (CISA), *Cost of a Cyber Incident: Systematic Review and Cross-Validation* https://www.cisa.gov/publication/cost-cyber-incident-systematic-review-and-cross-validation. Released October 2020.

Case Study Scenario Supplement - Active Shooter Undesirable Event

A former employee gained access to the lobby area through the congested entrance. Once in the lobby, the individual carried out an armed assault killing three people, severely injuring two, and moderately injuring one.

To calculate the consequence of a UE where human injuries or loss of life occur, multiply the number of fatalities by the VSL of $11.6 million. Then multiply the cost per "averted injury by type of injury (AIS Code)" by the number of each type of injury.

According to DOT recommendations (Table 1, p. 23), a disutility factor of 26.6 percent applies for severe injuries, which results in a cost of $3.09 million per non-chemical severe injury ($11.6 million × 26.6% (.266)). DOT recommends using 4.7 percent for moderate injuries, which results in a cost of $0.55 million per non-chemical moderate injury ($11.6 million × 4.7% (.047)). Under the AIS, examples of severe injuries include a spleen rupture or a chest-wall perforation, and examples of a moderate injury includes a major abrasion or laceration of skin.[1] Table 2 demonstrates calculation of the consequences associated to the case study's active shooter UE. While this scenario does not address property damage, law enforcement response, clean-up, and rescue costs, a breakeven may also account for these types of direct costs. Keep in mind the cost per averted fatality or injury comes from the AIS codes found in Table 1. Note: Calculations may not be exact in table due to rounding displayed values.

Table 2: Case Study Scenario - Active Shooter UE Scenario Consequence Cost

Types of Averted Impacts	Number of Averted Fatalities or Injuries	Cost per Averted Fatality or Injury (millions)	Total Cost (millions)
	a	b	c = a × b
Fatalities	3	$11.6M	$34.80
Severe Injuries	2	$11.6M x .266 = $3.09	$6.17
Moderate Injuries	1	$11.6M x .047 = $0.55	$0.55
Total Consequences			**$41.52**

Figure 12: Case Study – Active Shooter Undesirable Event with VSL Calculation

The next step in the breakeven analysis is to estimate how often the attack would need to be averted for the expected benefits to equal estimated costs. To conduct the breakeven analysis, compare the estimated monetary costs of an attack to the annualized cost of the proposed security measures. However, before estimating, follow these steps:

- Verify costs for the proposed security measure are annualized.
- Assume the proposed security measure cost is $596,033 (see Figure 11).
- Convert these security measure costs into millions to compare to the attack consequence costs also in millions. For this example, the annualized cost is $0.60 million.
- Divide the cost of a successful attack ($41.52) by the annualized cost of security measures ($0.60).

Table 3 provides the breakeven results associated with the case study. In this hypothetical scenario, based on the consequence cost and the total cost of the preferred option over the 10-year lifecycle, the preferred option would need to prevent an attack once every 70 years. Although organizations do not know the total number of UEs that will occur or be deterred, organizations can say how many incidents

the mitigation measures would need to prevent for the costs of the measure to break-even with the benefits of avoiding the costs of those UEs. For this reason, the VSL Calculation can be used for determining non-quantified benefits when performing a breakeven analysis.

Table 3: Case Study Scenario – Active Shooter Breakeven Results

Security Measure	Direct Cost of a Successful Active Shooter (millions)	Annualized Cost of Proposed Option (millions)	Break-Even Averted Attack Frequency
	a	b	c = a ÷ b
Proposed Option	$41.52	$0.60	Once every 70 years

When this break-even occurs, the security measures are cost-justified. Organizations must ensure research and evidence suggest a strong relationship between the security measures and the reduction in risk of the respective UE used in the breakeven analysis. It is important to state why a particular alternative would be rejected or preferred when evaluating alternatives. Presumably the lower cost alternative would provide less security value or have a lower likelihood of mitigating the risk.

Examples of indirect consequences can include the enactment of new laws, policies, and risk mitigation strategies or investments, as well as long-term cleanup efforts. Indirect consequences are important because they may have greater and longer-lasting effects than the direct consequences. Indirect consequences are more challenging to quantify and may need to be described qualitatively. Though the cost of remediating a physical or cyber incident may be quantifiable, recovering an agency's damaged infrastructure and/or reputation can be difficult to assess. There is no substitute for the public's trust, which is an indirect cost difficult to quantify.

6.2.8.2 Non-Quantifiable Table of Benefits

When making a business case for security, it may be useful to show non-quantifiable benefits in terms of security and non-security specific benefits. A list of non-quantifiable benefits would be documented in a detailed explanation within the life-cycle cost analysis with strong qualitative statements. Organizations may list-rank non-quantifiable benefits (similarly to quantifiable) for each alternative based on their relevance to the objective and the analysis. Table 4 provides examples of benefits from the case study.

Table 4: Case Study Scenario: Non-Quantifiable Table of Benefits

Security Specific	Non-Security Specific

• Reduction of overall risk
  ○ Reduced target attractiveness
  ▪ Fewer visitors and less exposure time in non-screened area
  ▪ Hardened target
  ○ Reduced vulnerability
  ▪ Increased detection capabilities
  ○ Reduced consequence
  ▪ Reduced number of potential casualties
  ▪ Increased survivability and response by security force
  ▪ Create redundancy in screening
	• Enhanced customer experience
	• Improved public reputation
	• Increased feelings of safety by employees

6.2.9 Characterize Uncertainty in Benefits, Costs, and Net Benefits

Uncertainty is inherent in any forecast of future conditions. Analysts should attempt to characterize the sources and nature of and limitations due to uncertainty. Organizations should develop a list of potential assumptions and/or scenarios to analyze the impact uncertainty may have on the baseline and alternative options. For example:

- How long is the security equipment expected to last with proper maintenance?
- What is the outlook from the Design Basis Threat (DBT) Report on the specified UE?
- How long is the organization expected to remain at the current location?
- Are there projected changes in the organizational mission?

6.3 U.S. Army Cost Benefit Analysis Guide

The OMB methodology is not the only method available. Organizations should also review other methods, such as the US Army Cost Benefit Analysis Guide (CBA). The stated goal of the CBA is to "make the cost benefit analysis process as clear and user-friendly as possible." Designed and implemented to address "constrained resources", Table 5 notes key elements in the CBA organizations may find valuable.

Table 5: Key Takeaways of the Army CBA

Tangible	Intangible	Financial

• Seeks to find an unbiased solution
• Provides examples throughout
• Clearly states the objectives of each step
• Reviews key principles at the end of each step
• Defines alternatives and courses of action (COAs) and the five screening categories: suitability, feasibility, acceptability, distinguishability, and completeness
• Considers second and third order effects (positive and negative) of each COA
• Offers links to internal tools used to build a BCA
• Breaks down cost analysis process by establishing the ground rules, assumptions, data collection and analysis, and WBS to get a cost estimate which is reviewed for accuracy, reasonableness, and sensitivity
	• Encourages teams of subject matter experts (SMEs) to build BCAs and promotes brainstorming of ideas
	• Recognizes the positive contributions of qualitative benefits
	• Enables the use of a quantitative approach for weighing qualitative benefits in the absence of quantitative measures
	• Uses visual depictions rather than complicated formulas for comparison charts
	• Uses a decision matrix to evaluate non-financial criteria scoring and a simplistic approach to combine financial and non-financial criteria
		• Provides numerous sources for cost estimating
		• Compares benefits, costs, and risk in the form of probability and impact assessment
		• Narrows down the number of alternatives and costs prior to developing indirect and direct cost estimates
		• Views quantifiable benefits (financial) as:
		  ○ Cost reduction
		  ○ Savings
		  ○ Cost avoidance
		  ○ Revenue generation
		  ○ Productivity improvements

7.0 Selecting Cost-Effective or Alternative Solutions

The OMB recommends organizations compare up to four separate options. These include the baseline (status quo), with the preferred option, a more stringent and less stringent alternative, and the benefits and costs of the possibilities.[16] The selection process should reflect the full spectrum of benefits and costs to include maintenance, firmware/software upgrades, and life-cycle replacement.

There are some instances where an organization would not make the selection through a comparative analysis of alternatives. An example is when the facility security committee (FSC) or tenant representative for single-tenant facilities, (hereafter referred to as "responsible authority"), are following the RMP and determining the achievable level of protection (LOP). In such cases, the responsible authority works with the security organization to identify a less stringent alternative in the form of the highest achievable level of protection through an iterative process of examining countermeasures identified in the RMP, Appendix B, *Countermeasures*.

8.0 Application within the Risk Management Process

The RMP defines the criteria and processes those responsible for a facility's security should use in determining a facility's security level and necessary LOP. This standard provides an integrated, single source of physical security countermeasures and guidance on countermeasure customization for all non-military federal facilities. The RMP identifies an achievable LOP commensurate with—or as close as possible to—the level of risk without exceeding the level of risk. To accomplish this, the RMP outlines the six-step approach shown in figure 13.

Figure 13: The ISC Risk Management Process

[16] Office of Information and Regulatory Affairs, OMB "Circular A-4: Regulatory Impact Analysis: A Primer" https://www.reginfo.gov/public/jsp/Utilities/circular-a-4_regulatory-impact-analysis-a-primer.pdf

8.1 Risk Assessments

The RMP requires risk assessments for federal facilities to be conducted by the facility's security organization once every five years for Facility Security Level[17] (FSL) I and II facilities and once every three years for FSL III, IV, and V. Therefore, it is advisable to include security organizations early in the planning and design process for construction or modernization projects. In addition to the risk assessment, security organizations are responsible for recommending appropriate countermeasures. The responsible authority is required to either implement the recommendations or to accept risk as part of the facility risk management strategy.

The RMP places an emphasis on assessing cost-effectiveness and measuring performance as part of a rigorous risk management approach for effective resource allocation.[18] When a vulnerability is identified and a risk mitigation strategy recommended, a decision must be made by the responsible authority to either proceed with the recommendation, implement an alternative (lower level) countermeasure, or accept the risk. In such instances, developing a business case for security with a BCA may be a valuable tool in getting the resources necessary to implement the appropriate risk mitigation strategy. The development of the BCA would occur during RMP Step 4: Determine Necessary or Achievable LOP. If the responsible authority decides to accept the risk, the analysis and effort to make the business case for security may be useful during the next budget cycle or other funding opportunities in the future.

Organizations may also find a BCA useful in non-traditional ways to support policy related countermeasures. For example, issuance of personal identification verification (PIV) cards to employees requires staffing. Organizations will need to determine whether the staffing will be provided by current employees or if additional employees will be needed. If an organization opts for additional staffing, then development of a sound business case should help the organization obtain the necessary resources to implement their plans.

[17] A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of countermeasures specified in ISC standards.

[18] *GAO-15-444 Action Needed to Better Assess Cost Effectiveness of Security Enhancements at Federal Facilities.*

9.0 Measuring Success

Measuring success is central to ensuring security organizations can demonstrate a positive ROI to leadership. When measuring success of a business case for security, most organizations will focus on qualitative or quantitative measurements. For example, quantifiable benefits are financially based and can measure cost avoidance, cost reductions, or cost savings. Conversely, non-quantifiable attributes can represent intrinsic values such as morale, satisfaction, or quality.

The following references provide organizations details on developing performance measures:

- The Risk Management Process, An ISC Standard - Appendix E: Use of Performance Security Measures
- Interagency Security Committee Compliance Benchmarks, FOUO, (2019)
- Government Performance and Results Act (GPRA) of 1993 and the Government Performance and Results Act Modernization Act (GPRAMA) of 2010.
- Government Accountability Office (GAO), GAO-06-612, "Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts", (May 2006).
- United States Environment Protection Agency (EPA) / National Center for Environmental Innovation (NCEI), Guidelines for Measuring the Performance of EPA Partnership Programs (June 2006), https://www.epa.gov/sites/default/files/2015-09/documents/guidelines-measuring-epa-partnership-program.pdf.
- U.S. Environmental Protection Agency (EPA) / National Center for Environmental Innovation's Guidelines for Measuring the Performance of EPA

9.1 Performance Measures

To develop a performance measurement, first determine the specific objectives or goals by articulating "what success looks like". Secondly, identify the performance measurement category, and lastly, outline what specific actions or measures will be taken.

Regardless of which type of benefit is used to measure success, the organization must first know their baseline for comparison. Once a baseline is established, the measures are queried again at a set time (after the approved security option is established/installed), to see if any changes can be observed. Table 6 provides an example of some performance measurements used to support a business case.

Table 6: Case Study: Performance Measurements

Objective/Goal	Measurement Category	Performance Measurement

Reduce risk to visitors/employees in unscreened areas	Quantitative	• Compare pre/post installation of new security measures in the following areas:
		  ○ Is there a reduction in volume of personnel outside screened areas?
		  ○ Is there a reduction of time of exposure for personnel outside screened areas?
		  ○ Are there fewer reported incidents/complaints between staff and visitors from co-mingled access?
		• Compare number of incidents in lobby to include reviewing ACSO reaction times and how quickly an incident was resolved with the limited congestion of crowds.

Improve business productivity	Quantitative	• Compare number of missed appointments. • Compare staff productivity due to eliminating gaps between appointments.

Enhance customer satisfaction and organization reputation	Non-quantitative	• Provide visitor satisfaction survey before and after queuing lines are expanded
		• Provide employee satisfaction survey after renovations to determine if:
		  ○ Completing business actions quicker positively or negatively affects the workforce.
		  ○ Tenants believe the dedicated employee lines create a more efficient and **safe** entry into the facility.

Appendix A: Factors for Identifying Alternatives

FACTOR	WHAT TO CONSIDER	EXAMPLE SCENARIO: ***An organization is considering installation of a new or upgraded ESS.***
RESOURCE SOLUTIONS	Similarly situated problems across business or critical infrastructure sectors with identified solutions. [Note: The National Institute of Standards and Technology (NIST) provides guidance to the private IT sector for similarly situated problems in the government.] Reviewing best practices, white papers, or other related periodicals/reports from private and public sector resources to determine existing solutions to similar problems.	Review federal information resources on access control and electronic security system design, implementation, and execution to understand the minimal requirements, best practices, and other factors.
VENDOR-ORIENTED APPROACHES OR ALTERNATIVE FUNDING OPTIONS	Contract and/or vendor-oriented approaches to achieve goals, potentially affording entities greater flexibility in compliance such as contracting personnel, services, or equipment. Alternative funding options such as modernization or efficiency funds managed by federal partners.	Consider contracted services such as design, installation, maintenance, and how vendor approaches impact costs and cost savings over time.

FACTOR	WHAT TO CONSIDER	EXAMPLE SCENARIO: ***An organization is considering installation of a new or upgraded ESS.***
OBJECTIVE BASED, PERFORMANCE BASED, OR SPECIFIC SERVICES TO BE PERFORMED	Federal Acquisition Regulations (FAR) to determine if solicitation documentation should be performance or objective based.[19] A statement of objectives (SOO), which is a government-prepared document incorporated into the solicitation stating the overall performance objectives. An SOO is used when the government intends to provide maximum flexibility to each offeror to propose an innovative approach. A performance work statement (PWS), which is a statement of work for performance-based acquisitions describing the required results in clear, specific, and objective terms with measurable outcomes.	During acquisition development, consider outcome-based solicitations or detailed performance-based requirements solicitations. Evaluation of each type of contract may include the federal representative's level of expertise and time available to manage the contract. Consideration of acquisition options could result in cost efficiencies and cost-effective alternatives.

[19] https://www.acquisition.gov/

FACTOR	WHAT TO CONSIDER	EXAMPLE SCENARIO: ***An organization is considering installation of a new or upgraded ESS.***
MINIMUM STANDARDS AND REQUIREMENTS BASED ON SIZE	Minimum action necessary to solve a problem or satisfy a requirement. Size and scope necessary to solve a problem or satisfy a requirement. [Note: If the expected cost and benefit vary based on the size and scope of alternative actions, an estimation of the differences should be considered.] Time associated with implementation based on the identified size and scope.	Referencing the risk assessment, consider the minimum requirements for the project, which are usually determined by the RMP, and customize them based on facility attributes. Local attributes of the facility or site of the reader may impact the type or need for equipment. Factors such as the type and number of badge readers meeting or exceeding minimum standards should be considered in developing alternatives. *Examples: 1) When considering badge readers within a facility, one may need to consider traffic at the reader location. In a high traffic entry point, there may be benefits from a higher cost investment for a more durable reader. However, a low traffic entry point with a less expensive reader may still meet the needs.* *2) Whether to include swipe and pin entry for multi-factor authentication (MFA), which increases security but may have higher cost and delay entry throughput. These factors should be part of the prior facility risk assessment; if they were not, consider an additional risk assessment to make the determination on such alternatives.*

FACTOR	WHAT TO CONSIDER	EXAMPLE SCENARIO: ***An organization is considering installation of a new or upgraded ESS.***
PERFORMANCE MONITORING, ENFORCEMENT METHODS, AND STRINGENCY	Benefits and costs associated with implementing performance monitoring programs, quality assurance programs (contract evaluation), and enforcement methods (on-site inspections and/or audits, periodic reporting, and noncompliance penalties). Benefits and costs regarding the level of stringency associated with implementing performance monitoring or enforcement methods.	Test equipment at certain intervals and monitor functionality on a pre-determined basis. Consider special equipment required to maintain the equipment, such as maintenance lift stands to replace burned out lighting or other maintenance of cameras, and if maintenance will be performed by current maintenance staff or outsourced.
IMPLEMENTATION DATES	Dates associated with implementation; the more time an agency has to identify solutions or options, the greater the opportunity to reduce costs while maximizing benefits. Risk trade-offs for delaying implementation or stages when evaluating alternatives.	Extending the implementation date may provide additional benefits such as more time for research and coordination to get more cost-effective equipment with increased benefits. There may be benefits in additional equipment testing upon installation. However, testing and resolution could extend the timeline if it was not accounted for in the project work plan. The application of different types of readers and cameras with different life cycles should be considered in estimating alternative costs.

FACTOR	WHAT TO CONSIDER	EXAMPLE SCENARIO: ***An organization is considering installation of a new or upgraded ESS.***
REQUIREMENTS BASED ON GEOGRAPHIC AND OTHER LIMITATIONS	Implementing alternative actions for different regions to maximize net benefits if there are significant regional variations in benefits and/or costs. An example of other limitations is public access to facilities. Federal facilities supporting the public through open access to their facilities may not be able to fully implement restrictive countermeasures or security enhancements.	Areas prone to storms and natural hazards may require additional redundancies, secondary power supply, or other mitigation measures. Consideration of geographic impacts or other limitations should also be included in alternatives. For cameras, consider lighting at the site and account for additional lighting or specialized cameras in certain conditions as well as weather for outdoor cameras and equipment.

Appendix B: Labor Rate Calculation

When acquisition or historical labor rates are unavailable, organizations may use federally published data to estimate wages and benefits. Begin by identifying labor categories and occupation types and industry per the Bureau of Labor Statistics' (BLS) National Wage Data. BLS wage data by area and occupation are available from the National Compensation Survey, Occupational Employment Statistics Survey, or the Current Population Survey.[20]

To the extent practicable, account for benefits and other costs in non-federal labor costs. BLS also provides data on wages, salaries, and other employee costs, (employee health and retirement benefits) in the Employer Costs for Employee Compensation (ECEC) Reports[21]. The ECEC data can be used to calculate non-federal compensation factors, which account for benefits and employer costs in addition to wages. Using the appropriate ECEC data table, calculate the compensation factor based on the total compensation divided by the wages. This ratio, or compensation factor, can then be applied to respective wages to calculate a compensation rate or loaded wage rate. The following example demonstrates the calculation of a compensation rate (wages and benefits):

> Figure 14 assumes private industry workers compensation costs on average $37.24 per hour and wages an average of $26.36 per hour. To calculate a compensation factor, divide $37.24 by $26.36 to get $1.412747. Then if a cost estimate for the security requirement labor has an identified wage rate, multiply it by the compensation factor to get a compensation rate. For example, assume security labor for the project is an estimated wage of $30.00 an hour, multiply $30.00 by 1.412747 to get a $42.38 compensation rate per hour. The following table displays the calculations.

Private Industry Worker-Hourly Compensation	Private Industry Worker-Hourly Wages	Compensation Factor	Security Labor-Hourly Wage	Security Labor Hourly Compensation
$37.24	$26.36	$37.24 ÷ $26.36 = 1.412747	$30.00	1.412747 × $30.00 = $42.38

Figure 14: Example Calculation of Compensation (Loaded) Labor Rate

When using ECEC, there may be more specific wage and compensation data for the cost estimate compared to the national private industry average; refer to BLS websites for more information. Additionally, part-time and full-time workers frequently have different compensation factors and may need to be factored into the cost estimate.

[20] Overview of BLS Wage Data by Area and Occupation : U.S. Bureau of Labor Statistics https://www.bls.gov/bls/blswage.htm and National Occupational Employment and Wage Estimates (bls.gov) https://www.bls.gov/oes/current/oes_nat.htm

[21] Employer Costs for Employee Compensation - 2021 Q04 Results (bls.gov) https://www.bls.gov/news.release/ecec.toc.htm

Appendix C: Additional Details to Quantify and Monetize the Benefits and Costs

Costs for Operations & Sustainment (O&S)

Direct operations and acquisition of resources (AOR) include costs to procure equipment and materials. Prior to proposal and estimation, consult with the agency's office of acquisition or local acquisition representatives. Request available procurement office guidance, if available. Examples could be cost to procure contracted security services,[22] labor, training, administrative, and personnel equipment costs.[23]

Personnel or Support Labor Costs

When estimating labor or personnel costs, consider staffing, wages, grade classifications, and other entitlements such as employee benefits. In addition to security personnel performing duties, consider supervision, management, and administrative support labor costs. Depending on the type of labor, federal or non-federal, the source for labor cost data and assumptions will vary. Also consider geographic and local wages versus national averages, whenever possible. If the costs are specific to a location(s), account for locality pay rates using the Office of Personnel Management website on base rates.[24]

Use prorated labor costs when federal or non-federal employees are not spending 100% of their time on the proposed activity. For example, if a GS-13 Step 5 position spends 20% of their time performing an estimated function, the prorated cost is the entered 0.2 FTE of the GS 13 Step 5. In other federal wage systems, it may be beneficial to use the mid-grade or mid-band level for pay-banded systems. If agency specific information regarding civilian compensation is unavailable, one may use a fringe benefit-cost factor of 36.25% of a position's basic pay.[25] The 36.25% civilian position full fringe benefit cost factor is the sum of the standard civilian position retirement benefit-cost factor, insurance and health benefit cost factor, Medicare benefit-cost factor, and miscellaneous fringe benefit-cost factor. Whenever possible, seek agency-specific guidance on the personnel benefits factors as there may be variation in factors based on the agency or position type. [Note: Basic pay for federal wage system positions is the position's annual wages including shift differential pay and environmental pay plus any applicable "other civilian pay entitlements".] Finally, personnel costs should include replacement of personnel lost through attrition and replacement personnel hiring and training costs.

When estimating commercial or industry labor rates, it may be beneficial to consult acquisition specialists to provide hourly rates for equivalent labor. Consider the level of necessary experience, licensing, and other technical skills necessary for more accurate labor rates. When historical and acquisition information are unavailable for commercial or industry labor rates, Appendix B provides an alternate method to calculate wages and benefits (accounting for the full cost of labor).

---

[22] Interagency Security Committee, *Best Practices for Armed Security Officers in Federal Facilities*

[23] It is mandated within GSA controlled/leased space that all contract guards be vetted through Federal Protective Services (FPS); in space independently leased by a federal department/agency, it is recommended that the lessor adhere to established internal department/agency policies and ISC best practices.

[24] OPM, Salary and Wages

[25] OMB, Update to Civilian Position Full Fringe Benefit Cost Factor, Federal Pay Raise Assumptions, Inflation Factors, and Tax Rates used in OMB Circular No. A-76, "Performance of Commercial Activities" March 2008

Information Technology Costs

Consider the cost of post-production software support and software services/license renewal. When looking at software, whether it be Software as a Service (SaaS) in a cloud environment or software in a physical environment as Operations and Maintenance (O&M) and Development, Modernization, and Enhancement (DME), special attention should be given to evaluating web service applications in general or cloud space (Software as a Service, Infrastructure as a Service, Platform as a Service, etc.).

Preventative Maintenance and Repair: IT and Equipment Costs

In addition to purchase and installation costs for equipment and software, consider preventative maintenance and repair estimates. Preventive maintenance is routine care designed to avert more costly repairs.[26] Consider if a regular maintenance cycle increases the life-cycle and performance of products and the life-cycle costs of leasing versus purchasing equipment.

Other Recurring or Incidental Costs

Other recurring or incidental costs include:

- Spares, necessary tools, and diagnostic equipment
- Renewal costs for items and supplies like batteries, bulbs, or gloves
- Site preparation, activation, movement, deployment, and testing for installation
- Construction costs for alteration or repair of facilities, structure, or other real property
- Inactivation or decommission of older equipment and life cycle of the new equipment

Contracting and Procurement Costs

As the primary acquisition and procurement arm of the federal government, GSA offers equipment, supplies, telecommunications, and integrated information technology solutions to federal agencies.[27] The GSA Federal Acquisition Service (FAS) can assist with general acquisition information, materials research, and Requests for Information, etc. Also, the FAS can aid with defining scopes for technology in a variety of applications. Agencies should conduct due diligence on researching and evaluating the systems and equipment procured within their respective agency. Consider consulting with GSA on their market research capability. The new services use robotic process automation to complete extensive research in GSA's data on products and services. GSA also provides specific information with a focus on building security. [28]

The GSA Blanket Purchase Agreements (BPAs) may offer improved, pre-negotiated terms and conditions for commercial off the shelf (COTS) software. BPAs can reduce risks and costs while saving administrative time and reducing paperwork. A GSA Schedule BPA is an agreement established by a government buyer with a Schedule contractor to fill repetitive needs for supplies or services.

---

[26] *ISC, Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* https://www.cisa.gov/publication/isc-resource-management-guide

[27] www.GSAAdvantage.gov

[28] www.gsa.gov/buildingsecurity; www.gsa.gov/federalprotectiveservice

Appendix D: Discounting

When comparison of options spans multiple years such as life-cycle costs, begin the analysis with base year dollars (constant dollars) compared to future year dollars. Normalize cost totals over a given length of time by converting them to constant dollars or discounting them using an appropriate discount rate. A discount rate may be reported as a percentage and assesses how much an agency prefers to spend on resources now instead of in the future. Discounting can be applied to compare the benefits and costs of the alternatives. Discount rates should be consistently applied between alternatives and the proposed action as well as on quantified benefits, if available. Timelines and horizons of the BCA should capture fluctuations in benefits and costs over time. The following table demonstrates discounting using 7% on a fictitious project cost estimate.

Table 7: Discounting Cost Examples Scenario 1

Not Delaying Costs										
		Year = t	**1**	**2**	**3**	**4**	**5**	**6**	**Total Present Value**	**Annualized Discounted Payments**
Discounting Factor	**7%**	$a_t = 1 \div (1 + 0.07)^t$	0.9346	0.8734	0.8163	0.7629	0.7130	0.6663		
Applying Discount Factors	**Costs Undiscounted**	b	$10,000	$1,000	$1,000	$1,000	$1,000	$10,000	**$24,000**	
	Costs at 7% Discounted	$c = a_t \times b_t$	$9,346	$873	$816	$763	$713	$6,663	**$19,175**	**$4,023**

Notes:

1. The total undiscounted cost is $24,000. The present value is the total amount a series of future payments is worth now.
2. Annualized payments are constant payments based on a constant discount rate over a specified period. One method to calculate the annualized payment is to use Microsoft Excel's PMT function. In this table, the PMT for the 7% discount rate is = -PMT(rate, number of payment periods or six years, present value or total costs discounted at 7%) or with values = -PMT(0.07, 6, $19,175) = $4,023.

An organization may consider a timeline with delayed implementation and costs incurred in the future. The evaluation of discounted costs provides a comparison of the two options. For example, the 7% discounted the annualized payments for Scenario 2 ($3,385) shown in Table 8 (below) are less than 7% discounted annualized payments ($4,023) for Scenario 1 in Table 7 (above).

Table 8: Discounting Cost Examples Scenario 2, Delaying Costs

Delaying Costs										
		Year = t	**1**	**2**	**3**	**4**	**5**	**6**	**Total Present Value**	**Annualized Discounted Payments**
Discounting Factor	**7%**	$a_t = 1 \div (1 + 0.07)^t$	0.9346	0.8734	0.8163	0.7629	0.7130	0.6663		
Applying Discount Factors	**Costs Undiscounted**	b	$0	$0	$0	$1,000	$1,000	$22,000	**$24,000**	
	Costs at 7% Discounted	$c = a_t \times b_t$	$0	$0	$0	$763	$713	$14,660	**$16,135**	**$3,385**

Discounting is a method used for the analysis of time-preference of spending. [Note: Use current year dollars instead of discounted costs when presenting official or financial accounting costs for budget and acquisition purposes.]

Appendix E: Resources
E.1: Acronyms

ACSO	Armed Contract Security Officer
AIS	Abbreviated Injury Scale
AOR	Acquisition of Resources
APA	Administrative Procedure Act
BCA	Benefit-Cost Analysis
BLUF	Bottom Line Up Front
BLS	Bureau of Labor Statistics
BPA	Blanket Purchase Agreements
BSC	Building Security Committee
BY	Base Year
CBA	Cost Benefit Analysis
CISA	Cybersecurity and Infrastructure Security Agency
COA	Course of Action
COTS	Commercial Off the Shelf
DHS	Department of Homeland Security
DME	Development, Modernization, and Enhancement
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
ECEC	Employer Costs for Employee Compensation
EO	Executive Order
EPA	Environmental Protection Agency
ESS	Electronic Security Systems
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FAS	Federal Acquisition Service
FPS	Federal Protective Services
FSC	Facility Security Committee
FSL	Facility Security Level
GAO	Government Accounting Office
GPRA	Government Performance and Results Act
GPRAMA	Government Performance and Results Act Modernization Act
GSA	General Services Administration
HHS	(Department of) Health and Human Services
HSPD	Homeland Security Presidential Directive
ISC	Interagency Security Committee
IT	Information Technology
LCCE	Life-Cycle Cost Estimate
LOP	Level of Protection
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
O&S	Operations and Sustainment
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management of Budget
PMBOK	Project Management Body of Knowledge

PIV	Personal Identification Verification
PWS	Performance Work Statement
RFQ	Request for Quote
RIA	Regulatory Impact Analysis
RMP	Risk Management Process
ROI	Return on Investment
SaaS	Software as a Service
SOO	Statement of Objectives
SOW	Statement of Work
TY	Then Year
UE	Undesirable Event
VSL	Value of Statistical Life
VSS	Video Surveillance System
WBS	Work Breakdown Structure
WTP	Willingness to Pay

E.2: Glossary

TERM	DEFINITION
Acceptable Risk	Acceptable risk describes the likelihood of an event whose probability of occurrence is small, whose consequences are so slight, or whose benefits (perceived or real) are so great, individuals or groups in society are willing to take or be subjected to the risk the event might occur. Extended definition: Level of risk at which - given costs and benefits associated with risk reduction measures - no action is deemed to be warranted at a given point in time. Example: Extremely low levels of water-borne contaminants can be deemed an acceptable risk.
Alteration	A limited construction project for an existing building comprised of the modification or replacement of one or several existing building systems or components. An alteration beyond normal maintenance activities but is less extensive than a major modernization.
Benefit-Cost Analysis (BCA)	A systematic quantitative method of assessing the desirability of government projects or policies when it is important to take a long view of future effects and a broad view of possible side-effects.
Break-Even/ Threshold Analysis	Variant of cost-benefit analysis estimating the threshold value for an uncertain parameter and equates to costs and benefits.
Building	An enclosed structure (above or below grade).
Building Entry	An access point into, or exit from, the building.
Business Case for Security	A decision-making process or rationale for proceeding with a security project or security program.
Campus	Two or more federal facilities contiguous and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be referred to as a “federal center” or “complex”.
Consequence	The level, duration, and nature of loss resulting from an undesirable event. Extended definition: Effect of an event, incident, or occurrence. Annotation: Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment. See also: human consequence (health), economic consequence, mission consequence, psychological consequence, indirect consequence, and direct consequence.
Constant Dollars/Base Year	Constant purchasing power in terms of the dollar value in the base year of the CBA.

TERM	DEFINITION
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the U.S. the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Current Dollars	Monetary value reflecting the effects of inflation. Prior-year costs stated in current dollars are the actual costs incurred in those years. Future costs or savings stated in current year dollars are the projected values to be paid out in future years.
Current dollars (then-year (TY) dollars, inflated dollars)	Nominal dollars expressed in the value of their year of occurrence. Past costs are simply expressed as the actual amounts paid out, unadjusted for price changes. Future costs are expressed in amounts expected to be paid out in their year of occurrence. Current costs and benefits measure the future purchasing power of the dollars. More importantly, it accounts for future assumed inflation rates. Because DOD policy states all budget estimates must be in current dollars, costs estimate prepared using constant dollars will have to be converted to current dollars when building a budget.
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks.
Design-Basis Threat	A profile of the type, composition, and capabilities of an adversary.
Distributional Effect	The impact of a regulatory action across the population and economy, divided up in various ways (income groups, race, sex, industrial sector, geography).
Facility Security Committee (FSC)	A committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities. The FSC consists of representatives of all federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC will also include the project team and the planned tenant(s). The FSC was formerly known as the Building Security Committee (BSC).
Federal Facilities	Government leased and owned facilities in the United States (inclusive of its territories) occupied by federal employees for non-military activities.
Federal Tenant	A federal department or agency paying rent on space in a federal facility. See also single-tenant, multi-tenant, and mixed-multi-tenant.

TERM	DEFINITION
Information Technology	Any equipment, interconnected system, or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
Life-Cycle Cost Estimate (LCCE)	The estimated cost of developing, producing, deploying, maintaining, operating, and disposing of a system over its entire lifespan.
Major Modernization	The comprehensive replacement or restoration of virtually all major systems, tenant-related interior work (ceilings, partitions, doors, floor finishes), or building elements and features.
Necessary Level of Protection	The determined degree of security needed to mitigate the assessed risks at the facility.
New Construction	A project in which an entirely new facility is to be built.
Non-quantifiable Benefits	A benefit not lending itself to numeric valuation, such as better quality of services.
Opportunity Cost	The maximum worth of a good or input among possible alternative uses.
Performance Management	An ongoing process of communication between a supervisor and an employee occurring throughout the year and in support of accomplishing the strategic objectives of the organization.
Performance Measure	Regular measurement of outcomes and results generating reliable data on the effectiveness and efficiency of programs.
Physical Security	Portion of internal security concerned with physical measures designed to safeguard personnel; prevent unauthorized access to equipment, facilities, material, and documents; and defend against espionage, sabotage, damage, and theft.
Project	Any undertaking having a finite beginning and finite end to achieve a specific goal.
Project Management	Application of knowledge, skills, tools, and techniques to project activities to meet the project requirements.
Project Management Plan	Formal, approved document defining how the project is executed, monitored, and controlled.
Quantifiable Benefit	A numeric value, such as dollars, physical count of items, or percentage change benefit assigned to a benefit.

TERM	DEFINITION
Regulatory Impact Analysis (RIA)	A well-established and widely used approach for collecting, organizing, and analyzing data on the impacts of policy options for evidence-based decision-making. It provides an objective, unbiased assessment, which is an essential component of policy development, and considers both quantifiable and unquantifiable impacts. Along with information on legal requirements, general policy goals, the distribution of the impacts, and other concerns, it forms the basis of the ultimate policy decision.
Risk	A measure of potential harm from an undesirable event encompassing threat, vulnerability, and consequence.
Risk Acceptance	The explicit or implicit decision to not take an action that would affect all or part of a particular risk.
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.
Risk Management	A comprehensive approach to allocating resources for the protection of a facility and its assets and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and, when necessary, risk acceptance.
Risk Mitigation	The application of strategies and countermeasures to reduce the threat of vulnerability to, and/or consequences from an undesirable event. Extended definition: Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. Measures may be implemented prior to, during, or after an incident, event, or occurrence. Example: Through risk mitigation, the potential impact of the tsunami on the local population was greatly reduced. Annotation: Measures may be implemented prior to, during, or after an incident, event, or occurrence.
Site	The physical land area controlled by the government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed.
Undesirable Event	An incident adversely impacting facility occupants or visitors, operation of the facility, or mission of the agency.

TERM	DEFINITION
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit. Extended definition: Physical feature or operational attribute rendering an entity open to exploitation or susceptible to a given hazard; characteristic of design, location, security posture, operation, or any combination thereof, rendering an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. Extended definition: Characteristic of design, location, security posture, operation, or any combination thereof, rendering an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. Example: Installation of vehicle barriers may remove a vulnerability related to attacks using vehicle-borne improvised explosive devices.
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and - when necessary - risk acceptance. Extended definition: Process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. Annotation: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge while risk often cannot be eliminated, actions can usually be taken to reduce risk.

E.3: References Cited

Bureau of Labor Statistics

- Overview of BLS Wage Data by Area and Occupation: U.S. Bureau of Labor Statistics
- National Occupational Employment and Wage Estimates
- Employer Costs for Employee Compensation - 2021 Q04 Results

CISA

- "Cost of a Cyber Incident: Systematic Review and Cross-Validation"

DHS

- Best Practices for the Treatment of Statistical Life in U.S. Department of Homeland Security Regulatory Analyses

DOT

- Departmental Guidance on Valuation of a Statistical Life in Economic Analysis | US Department of Transportation

EPA

- Guidelines for Measuring the Performance of EPA Partnership Programs

Executive Orders

- Executive Order 12866
- Executive Order 13563

Federal Aviation Administration

- "Economic Values for FAA Investment and Regulatory Decisions, A Guide Final Report"
- *Guidelines for Regulatory Impact Analysis*. Appendix D

GAO

- GAO-15-444 Homeland Security: Action Needed to Better Assess Cost Effectiveness of Security Enhancements at Federal Facilities
- GAO-06-612 Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts
- GAO Cost Estimation and Assessment Guide

GSA

- www.GSAAdvantage.gov
- www.gsa.gov/buildingsecurity
- www.gsa.gov/federalprotectiveservice

ISC

- Making a Business Case – Cost Analysis Template
- *Armed Contract Security Officers in Federal Facilities, An Interagency Security Committee Best Practice*
- *ISC, Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide*

Office of Information and Regulatory Affairs, OMB

- "Circular A-4: Regulatory Impact Analysis: A Primer"
- Circular No A-4, Regulatory Analysis
- Circular A-4, Regulatory Impact Analysis Primer
- Circular No. A-76, "Performance of Commercial Activities" March 2008
- Circular A-94, Guidelines for Discount Rates for Benefit-Cost Analysis for Federal Programs

OPM

- OPM, Salary and Wages

Regulations

- Government Performance and Results Act (GPRA) of 1993
- Government Performance and Results Act Modernization Act (GPRAMA) of 2010
- 41 CFR Part 102-81 Physical Security

U.S. Army

- U.S. Army Cost Benefit Analysis Guide

E.4: Additional Resources

ASIS Foundation Convergence Report. "The State of Security Convergence in the United States, Europe, and India" *ASIS International.* 2019. https://www.asisonline.org/security-management-magazine/articles/2020/01/is-security-converging/.

"Benefit-Cost Analysis Tool. "*Federal Emergency Management Agency*. accessed August 28. 2020 https://www.fema.gov/grants/guidance-tools/benefit-cost-analysis.

Biddiscombe, Simon. "Cybersecurity Starts at the Top: Why the C-Suite Should Lead Mobile Security" *Forbes.* June 19. 2020. https://www.forbes.com/sites/forbestechcouncil/2020/06/19/cybersecurity-starts-at-the-top-why-the-c-suite-should-lead-mobile-security/#14c8fcf81b48.

Boberg, Nathan and Blakemore, Keith. "Make your Case" *ASIS International.* 2014. https://www.asisonline.org/security-management-magazine/articles/2014/06/make-your-case/?_t_id=8yEa3b8FuoYiSDOGiKOD8A==.

"Does Enhanced Security Improve Business Performance?" USC CREATE: Homeland Security Center, National Center for Risk and Economic Analysis of Terrorism Events University of Southern California, July 23, 2020.

Gibbons, Serenity. 2020. "Why Investing in Cybersecurity Makes Sense Right Now". April 9. 2020. https://www.forbes.com/sites/serenitygibbons/2020/04/09/why-investing-in-cybersecurity-makes-sense-right-now/#4ee0f12b3d22.

Meyer, Clair. "Q&A: How to Build a Better Business Case." *ASIS International.* 2020. https://www.asisonline.org/security-management-magazine/articles/2020/06/qa-how-to-build-a-better-business-case/.

"Recommended Practices for Safety and Health Programs." *Occupational Safety and Health Administration.* Accessed August 28. 2020. https://www.osha.gov/shpguidelines/.

"UP Templates Library." US *Center for Disease Control.* https://www2a.cdc.gov/cdcup/library/templates/.

Acknowledgments

The ISC would like to thank the participants of the ***Making a Business Case for Security:***

Making a Business Case for Security Working Group

Michael Harman
Chair
Department of Commerce

John Eskandary
Co-Chair
Federal Emergency Management Agency

Subcommittee Members

Nikisha Bailey
Health and Human Services

Matthew Barbieri
Department of Commerce

Justine Brown
National Institute of Standards and Technology

William Brown
Cybersecurity and Infrastructure Security Agency

Christopher Burley
Cybersecurity and Infrastructure Security Agency

Kevin Choate
General Service Administration

Roy Davis
Health and Human Services

Hayley Edmunson
Cybersecurity and Infrastructure Security Agency

Juan Estrada
Department of Homeland Security

Michael Flagler
Customs and Border Protection

Roger Hansel
Internal Revenue Service

Jerald Hunter
Internal Revenue Service

Aaron Lewis
Federal Protective Services

Denesh Malaveetil
Health and Human Services

Darrell Maximo
Cybersecurity and Infrastructure Security Agency

Mackenzie McGuire
Department of Commerce

Elizabeth Mester
Cybersecurity and Infrastructure Security Agency

Emma Plikerd
Cybersecurity and Infrastructure Security Agency

Christena Johnston-Pulliam
Cybersecurity and Infrastructure Security Agency

Craig Rademacher
Bonneville Power Administration

Jeffrey Rice
Office of Personnel Management

Jason Scyphers
Department of Homeland Security

Melanie Spears
Cybersecurity and Infrastructure Security Agency

Caitlin Stephenson
Cybersecurity and Infrastructure Security Agency

Eva Timas
Cybersecurity and Infrastructure Security Agency

Reginald Watkins
Customs and Border Protection

Shaina Wojciechowicz
Cybersecurity and Infrastructure Security Agency

Interagency Security Committee Staff

Daryle Hernandez, Chief

Ben Adame
Program Analyst

Jami Craig
Technical Editor

Scott Dunford
Senior Security Specialist

Chris York
Program Analyst