



**Joint Planning
and
Development Office**

**Security Annex
Concept of Operations
for the
Next Generation Air Transportation System**

Version 1.2

February 28, 2007

NextGen
Next Generation Air Transportation System
Joint Planning and Development Office



ANNEX: LAYERED, ADAPTIVE SECURITY OPERATIONAL CONCEPT FOR NEXTGEN

5000
5001

5002
5003

PREFACE

5004 The Joint Planning and Development Office (JPDO) is developing a concept of operations
5005 (CONOPS) for the Next Generation Air Transportation System (NextGen). The final version of
5006 the CONOPS will provide an overall and integrated view of NextGen operations in the 2025
5007 timeframe, including key transformations from today's operations. The overall document also
5008 identifies key research and policy issues that need resolution to achieve national goals for air
5009 transportation. The development of the CONOPS is an iterative and evolutionary process that
5010 will progress using input and feedback from the aviation community.

5011 This document provides the aviation community with a preview of the NextGen CONOPS and
5012 receive their comments for improvements. Details of the JPDO comment and review process can
5013 be found at the Tech Hanger at www.jpdo.aero. The full version of this document will include
5014 accepted comments for the NextGen concepts related to the following;

- 5015
- 5016 • Airport operations and mission support
 - 5017 • Air traffic management planning and mission support services
 - 5018 • Flight operations planning and mission support services
 - 5019 • Layered adaptive security services
 - 5020 • Network-enabled infrastructure services
 - 5021 • Shared situational awareness services
 - 5022 • Safety management services
 - 5023 • Environmental management services
 - Compliance, regulation, and harmonization services.

5024 Often, this document presents "aggressive" concepts that have not been validated but are
5025 envisioned as attainable goals to maximize benefits and flexibility for NextGen users of 2025
5026 and beyond. Many potential futures are possible, and much will depend on the insights gained by
5027 the evolution and increasing specificity of the CONOPS. Comments to refine these research
5028 issues are requested.

5029 The ensuing document, which is the full version of Chapter 6 of the NextGen CONOPS Version
5030 1.2, describes the entire concept of layered adaptive security at the same high level as other
5031 chapters.

TABLE OF CONTENTS

5032			
5033			
5034	PREFACE		1
5035	1 INTRODUCTION		1
5036	1.1 OVERVIEW		1
5037	1.2 NEXTGEN SECURITY MANAGEMENT AND COLLABORATIVE FRAMEWORK.....		2
5038	1.3 NEXTGEN SECURITY OPERATIONAL IMPROVEMENTS SUMMARY		3
5039	2 INTEGRATED RISK MANAGEMENT		5
5040	2.1 RISK MANAGEMENT PROCESS		6
5041	2.2 SECURITY RISK MANAGEMENT.....		6
5042	2.2.1 IRM—Secure People		7
5043	2.2.2 IRM—Secure Airports.....		7
5044	2.2.3 IRM—Secure Checked Baggage		8
5045	2.2.4 IRM—Secure Cargo/Mail.....		8
5046	2.2.5 IRM—Secure Airspace.....		9
5047	2.2.6 IRM—Secure Aircraft		10
5048	2.3 NEI-ENABLED INTEGRATED RISK MANAGEMENT COLLABORATION ENVIRONMENT		11
5049	2.4 RISK MANAGEMENT STRATEGY MONITORING AND FOLLOW-UP.....		12
5050	3 SECURE PEOPLE		13
5051	3.1 INTEGRATED RISK MANAGEMENT		13
5052	3.2 AUTHENTICATION AND CREDENTIALING		13
5053	3.2.1 Credentialing.....		14
5054	3.2.2 Passenger Authentication.....		14
5055	3.2.3 Aviation Industry Worker Authentication		15
5056	3.3 CHECKPOINT PERSON SCREENING		15
5057	3.4 CHECK POINT BAGGAGE SCREENING.....		16
5058	3.5 CONTINUOUS SURVEILLANCE AT CHECKPOINT/ACCESS SITES		17
5059	3.6 GLOBAL HARMONIZATION.....		18
5060	4 SECURE AIRPORTS		19
5061	4.1 IRM—SECURE AIRPORT		19
5062	4.2 AIRPORT FACILITIES		20
5063	4.2.1 Commercial (Passenger/Cargo) Airports.....		20
5064	4.2.2 Remote Terminal Security Screening		20
5065	4.2.3 General Aviation Airports.....		20
5066	4.2.4 Commercial Spaceports		21
5067	4.3 AIRSIDE		21
5068	4.3.1 AOA/SIDA		21
5069	4.3.2 Terminal Perimeter		21
5070	4.3.3 Terminal Airspace Security		22
5071	4.4 LANDSIDE		22
5072	4.4.1 Airport Public and Commercial Roadways and Parking Lots.....		22
5073	4.4.2 Terminal Departures Curb		22
5074	4.4.3 Terminal Entry Portal		23
5075	4.4.4 Airline Ticketing Kiosk/Counter		23

5076 4.4.5 Security Checkpoint..... 23

5077 4.4.6 Sterile Concourse..... 23

5078 4.4.7 International Arrival/Customs 23

5079 4.4.8 Airport Concessions, Food, and Beverage Security 24

5080 4.5 AIRPORT SECURITY CONTROL CENTER..... 24

5081 4.6 EMERGENCY RESPONSE AND RECOVERY 24

5082 **5 SECURE CHECKED BAGGAGE..... 25**

5083 5.1 INTEGRATED RISK MANAGEMENT 25

5084 5.2 CHECKED BAGGAGE SCREENING 26

5085 5.2.1 Screening..... 26

5086 5.2.2 Alarm Resolution Screening..... 26

5087 5.2.3 Threat Object Disposal 27

5088 5.3 CHECKED BAGGAGE SCREENING INSTALLATIONS 27

5089 5.3.1 In-Line Baggage Screening..... 27

5090 5.3.2 Nonintegrated and Standalone Baggage Screening 28

5091 5.3.3 Deployable Baggage Screening Operations..... 28

5092 5.4 GLOBAL HARMONIZATION..... 28

5093 **6 SECURE CARGO AND MAIL..... 29**

5094 6.1 INTEGRATED RISK MANAGEMENT 30

5095 6.2 SHIPPER CREDENTIALING..... 30

5096 6.3 SCREENING AND INSPECTION 31

5097 6.4 ALARM RESOLUTION 31

5098 6.5 SURFACE TRANSPORTATION SECURITY OF SCREENED CARGO..... 32

5099 6.6 HARDENED DOORS AND BARRIERS ON ALL CARGO AIRCRAFT 32

5100 6.7 SECURITY TRAINING FOR ALL CARGO FLIGHT CREW AND STAFF..... 32

5101 6.8 STORAGE SECURITY 32

5102 6.9 CARGO TRACKING AND INTEGRITY..... 32

5103 6.10 GLOBAL HARMONIZATION..... 32

5104 **7 SECURE AIRSPACE..... 34**

5105 7.1 INTEGRATED RISK MANAGEMENT 34

5106 7.2 VERIFIED AIRSPACE ACCESS 34

5107 7.3 SECURITY RESTRICTED AIRSPACES..... 35

5108 7.4 AIRSPACE VIOLATION DETECTION, ALERTING, AND MONITORING..... 36

5109 7.5 INTEGRATED MANAGEMENT OF AIRSPACE SECURITY..... 37

5110 7.5.1 Noncooperative Surveillance 37

5111 7.5.2 Countermeasures..... 37

5112 7.5.3 Joint Exercises 38

5113 7.6 COUNTER PROJECTILES..... 38

5114 7.6.1 Airport AOA/Terminal Airspace 38

5115 7.6.2 Aircraft/Flight Object..... 39

5116 **8 SECURE AIRCRAFT 40**

5117 8.1 INTEGRATED RISK MANAGEMENT 40

5118 8.2 AUTHORIZED CONTROL OF THE AIRCRAFT 40

5119 8.2.1 Cockpit Systems..... 40

5120 8.2.2 Onboard Personnel..... 40

5121	8.3	AIRCRAFT MONITORING/SURVEILLANCE	41
5122	8.3.1	Cockpit, Cabin, and Cargo Hold Surveillance.....	41
5123	8.3.2	Continuous Air Monitoring.....	41
5124	8.4	AIRCRAFT HARDENING AND DEFENSIVE SYSTEMS	42
5125	8.5	SAFETY INTEGRATION.....	42
5126			
5127			



LAYERED, ADAPTIVE SECURITY SERVICES (ENTERPRISE OPERATIONS)

5128
5129

5130

1 INTRODUCTION

1.1 OVERVIEW

5133 This concept of operations (CONOPS) for the Next Generation Air Transportation System
5134 (NextGen)¹ has incorporated an effective security system without unduly limiting mobility or
5135 making arbitrary intrusions on the civil liberties of all users by embedding layered, adaptive
5136 security measures throughout the air transportation system, from reservation to destination. This
5137 NextGen Security concept addresses the following: 1) Integrated Risk Management, 2) Secure
5138 People, 3) Secure Airports, 4) Secure Checked Baggage, 5) Secure Cargo/Mail, 6) Secure
5139 Airspace, and 7) Secure Aircraft.

5140 The security system has particularly strong interrelations with NextGen Shared Situational
5141 Awareness, airports, and global harmonization capabilities along with some aspects of Agile
5142 ATM. Cyber security is addressed in the Net-Centric Infrastructure Services, Chapter 4, and
5143 Shared Situational Awareness (SSA) Services, Chapter 5 of the Concept of Operations Version
5144 1.2 document. Non-cooperative surveillance is also addressed in Chapter 5 of the same
5145 document.

5146 Layered, adaptive security is defined as a risk-informed security system that depends on multiple
5147 technologies, policies, or procedures adaptively scaled and arranged to defeat a given threat. This
5148 adaptability further permits the use of increased variability in system operations that creates
5149 additional uncertainty for the terrorist. Adversaries cannot defeat one particular security measure
5150 and system and thereby achieve a “break-through,” which permits them to operate freely with no
5151 further barriers to their activities. Furthermore, the security system has the adaptability to scale
5152 its systems and procedures to the risk level of a threat in a given situation rather than being
5153 bound to an inflexible “one size fits all” approach.

5154 Given the limited resources of government and private industry, it is critical that mitigation
5155 measures be developed based on threat and vulnerability, as well as the potential consequences
5156 to individuals, transportation assets, and the economy.

5157 The NextGen approach better matches system costs with the risk assessment and the capacity
5158 demands at various airport and screening locations.

5159 To achieve the requisite adaptability while maintaining effective security standards, the NextGen
5160 security system must have a sound method of prioritizing risks and assessing the proportional
5161 effectiveness of different ways of countering them. The Secure-Integrated Risk Management
5162 process performs this essential function that then directs the deployment of equipment,

¹ The term “NextGen” in this document applies solely to the JPDO Enterprise Architecture and CONOPS for 2025. No other program is referenced or intended by this term.

5163 personnel, and procedures and policies to defeat the evolving threat. The remaining capabilities
5164 described at a high level in this chapter must be the consequence of integrated risk management
5165 (IRM) assessments.

5166 **1.2 NEXTGEN SECURITY MANAGEMENT AND COLLABORATIVE FRAMEWORK**

5167 In the NextGen, the security system is better integrated with other National Airspace System
5168 (NAS) functions, and through advanced networking functionality, linked to external aviation
5169 industry stakeholders and non-Federal government entities. To maintain effective security
5170 management across major stakeholders, a collaborative framework is composed of the following
5171 key functions and processes identified below.

5172 **National Aviation Security Policy.** NextGen security policy embraces a broad view of threats,
5173 including direct attack, exploitation, and transfer; recognizes interdependencies and uncertainty;
5174 nurtures virtual or extended enterprises supported by connectivity of diverse, informed
5175 stakeholder partnerships; employs layered security using physical, process, and institutional
5176 layers; accounts for systemic vulnerabilities that are created by the networked nature of the
5177 aviation system; and creates resilience in the system to mitigate potential incident consequence.
5178 The NextGen has achieved integration with the overarching Homeland Security Presidential
5179 Directives and their subsidiary documents.

5180 • **Aviation Security Stakeholder Involvement.** NextGen Stakeholder Involvement fosters
5181 industry, federal, and local partnerships with clearly defined roles and responsibilities for
5182 prevention, protection, response and mitigation, and recovery operations at strategic,
5183 operational, and tactical levels. Collaborative decision-making contributes to a positive
5184 security culture. Rapid decision-making based on shared situational awareness is
5185 achieved through advanced communication and information sharing systems.

5186 • **Integrated Risk Management.** NextGen IRM includes prognostic tools, models, and
5187 simulations at the strategic, operational, and tactical level to support all stakeholder
5188 decisionmakers and managers in the grafting of cost-effective “best practices” into the
5189 design, acquisition, deployment, and operation of aviation security system assets and
5190 infrastructures. Knowledge bases concerning threats, vulnerabilities, and practices are
5191 tailored to user profiles that proactively determine need/authorization to know.

5192 • **Aviation Security Implementation.** NextGen Implementation capabilities encompass a
5193 robust set of strategic, tactical, and operational capabilities and services focused on
5194 prevention, protection, response and mitigation, and recovery initiatives that are
5195 undertaken by various stakeholder organizations.

5196 • **Aviation Security Assurance.** NextGen Assurance capabilities include various
5197 certification programs administered by federal, industry, and local stakeholders,
5198 surveillance and evaluation activities administered and performed by various
5199 stakeholders, enforcement inspections performed by federal stakeholders and local
5200 stakeholders, and incident investigations performed and administered by various
5201 stakeholders.

5202 **1.3 NEXTGEN SECURITY OPERATIONAL IMPROVEMENTS SUMMARY**

5203 Table C-1 lists the major operational improvements that the NextGen Security system provides
5204 compared with the NAS of 2006.

5205 **Table C-1. Significant Security Transformations**

5206

Significant Transformation	2006 Current Capability	2025 NextGen Capability
Integrated Risk Management	<ul style="list-style-type: none"> Static facility or passenger risk assessments 	<ul style="list-style-type: none"> Dynamic risk assessment management process produces real-time risk profiles for aviation facilities and flight object.
Checkpoint Operations Responsibilities	<ul style="list-style-type: none"> US Government (USG)/TSA responsible for policy development and execution 	<ul style="list-style-type: none"> Government, airport operator, or third-party decentralized while observing common standards developed by USG
Credentialing/Authentication	<ul style="list-style-type: none"> Badges, background checks (mainly manual based) 	<ul style="list-style-type: none"> Biometric credentials with 1-second authentication at access or screening checkpoints
Baggage Screening Technology	<ul style="list-style-type: none"> Large footprint baggage screening devices—most not integrated with baggage system—only detect explosives. Separate boxes for chemical, biological, radiological, nuclear, and explosives (CBRNE) sensors 	<ul style="list-style-type: none"> CBRNE detection systems incorporating sensor fusion, with a range of sizes and throughput capacity from high throughput in-line systems to smaller units for remote screening, local airports. Some are small, lightweight, and portable devices that can screen bags from standoff distances.
Passenger Screening	<ul style="list-style-type: none"> Metal detector-based, relatively large explosive trace detection (ETD) air sampling equipment/portals 	<ul style="list-style-type: none"> Sensor arrays deployable throughout terminal enabling rapid movement of passengers through virtually invisible screening points—fast and efficient—centralized monitoring center reduces security footprint at checkpoint. Advanced behavior profile recognition (BPR) procedures. Biological threat and disease detection and assessment.
Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Detection	<ul style="list-style-type: none"> Only deployed at a few high-threat locations (typically not airports) 	<ul style="list-style-type: none"> Deployable for all airport screening operations, link by network-enabled infrastructure (NEI) to airport operations, law enforcement and national network
Security System Deployability	<ul style="list-style-type: none"> Expensive slow installation 	<ul style="list-style-type: none"> Rapid deployable units for low-capacity, temporary and intermittent screening locations integrated with other airport customer service functions

Significant Transformation	2006 Current Capability	2025 NextGen Capability
Screening Checkpoint Location	<ul style="list-style-type: none"> In airport terminals between public area and “sterile” area 	<ul style="list-style-type: none"> Remote Terminal Security Screening (RTSS) enabling all or portion of security screening to be conducted off-airport.
Man Portable Air Defense System (MANPADS) (e.g., shoulder-fired missiles, lasers, electromagnetic pulse [EMP]) Detection and Defeat	<ul style="list-style-type: none"> Perimeter and adjacent jurisdiction observation by law enforcement officers (LEO) 	<ul style="list-style-type: none"> Onboard aircraft leveraged safety modifications, supplemented by ground-based and procedural systems
Commercial Spaceport	<ul style="list-style-type: none"> Licensing with no commercial passenger service 	<ul style="list-style-type: none"> Passenger screening and bilateral agreements for international reentry of hypersonic vehicles
Security Relevant Information	<ul style="list-style-type: none"> Disparate, stand-alone systems; no easy transfer of data. 	<ul style="list-style-type: none"> Network-centric information access with “smart” applications proficient in data-mining and pre-analysis of large amounts of data. Decision support applications assist the security operations center and other security analysts.
Cargo Screening Technology	<ul style="list-style-type: none"> Small percentage of cargo being screened for explosive threats Most cargo undergoes paper-based documentation (known shipper) 	<ul style="list-style-type: none"> All air cargo items not packed in sterile area and securely conveyed to aircraft are screened for CBRNE.

5207

5208 2 INTEGRATED RISK MANAGEMENT

5209 Risk management is the ongoing process of understanding the threats, consequences, and
5210 vulnerabilities that can be exploited by an adversary to determine which actions can provide the
5211 greatest total risk reduction for the least impact on limited resources. Risk management is
5212 continuous; it is conducted from the strategic to the tactical levels. In this section, the strategic
5213 aspects of the IRM process are described. The following sections briefly mention the relevant
5214 tactical aspects of IRM for that particular threat vector. The NextGen layered, adaptive security's
5215 IRM capability is an overall federated risk assessment and risk mitigation framework for guiding
5216 multiple security service enterprises to assist in making decisions, allocating resources, and
5217 taking actions under conditions of uncertainty. This framework is a planning methodology that
5218 outlines the process for setting security goals through a) prevention, b) protection, c) response
5219 and mitigation, and d) recovery. It derives its importance from the following needs:

- 5220 • Understand the spectrum of threats that could be mounted against the NextGen.
- 5221 • Identify the vulnerabilities that can be exploited by an adversary.
- 5222 • Evaluate and prioritize assets and activities to be protected from attack.
- 5223 • Determine which protective actions can provide the greatest total risk reduction for the
5224 least impact on limited resources.
- 5225 • Provide the most focused and adaptive security measures to reduce the impact of security
5226 systems and procedures on air transportation.

5227 IRM is characterized by a specific and consistent terminology to describe its various aspects.
5228 Threats are the likelihood of a terrorist attack on a particular asset. Vulnerabilities are
5229 weaknesses in the design, implementation, or operation of an asset or system that can be
5230 exploited by an adversary or disrupted by a natural disaster. Consequences are the result of an
5231 attack on infrastructure assets reflecting level, duration and nature. Risks are measures of
5232 potential harm that encompasses threat, vulnerability, and consequence.

5233 The assessment of risks provides a prioritized list of vulnerabilities and potential mitigation
5234 strategies. The terrorist has freedom to choose targets and modes of attack; therefore, the
5235 NextGen Security system must develop (but not necessarily universally deploy) operationally
5236 feasible mitigations to as many potential threats as possible. Because of limited resources,
5237 mitigation requiring substantial investment (e.g., system cost or infrastructure intensive) is
5238 applied (deployed) in the order of risk level. For example, external attacks on aircraft may be an
5239 issue at some airports requiring mitigation. This does not mean that General Aviation airports
5240 will have or need such systems.

5241 Another way to stretch resources is through technical advances in sensor design and fusion and
5242 in cost efficiencies typical of information processing system upgrades. With the development of
5243 low-cost CBRNE sensors for low-volume operations, it is possible to conduct screening in 2025
5244 at sites that would have been economically infeasible in 2006 for a given risk profile (thus
5245 permitting many more airports to provide commercial service). This does not mean that all
5246 noncommercial operations need to screen passengers or cargo for flights posing below threshold
5247 risk levels. Many flight operations occur far from major metropolitan areas or national security
5248 restricted areas. However, flight operations to sensitive areas need to make adjustments to reduce
5249 their risk profile.

5250 In summary, it is essential to remember that the security system responses and procedures
5251 throughout the NextGen are applied based on the risk profile of each flight object and airport
5252 facility. Facilities or flights that do not adopt particular security processes may still operate in the
5253 *NextGen but may need to observe some restrictions depending on the given risk profile created.*
5254 *Yet, their overall access and performance in NextGen, even with some (self-imposed) security*
5255 *restrictions, is considerably greater than their access in 2006.*

5256 2.1 RISK MANAGEMENT PROCESS

5257 The primary objectives of the risk management process are evaluating the effects of defined
5258 threats, assessing the vulnerability, and evaluating and prioritizing assets and functions for a civil
5259 aviation system that is a significant target for our adversaries, including high-value localized
5260 targets. The IRM process divides risk management into phases:

- 5261 • Threat analysis
- 5262 • Vulnerability analysis and consequence assessment
- 5263 • Countermeasures definition
- 5264 • Countermeasures prioritization and acquisition strategy analysis
- 5265 • Procedural and technology insertion with subsequent evaluation.

5266 With the continuous review of threat vectors, objects, and materials, coupled with intelligence on
5267 current national threat levels, civil aviation passengers assure that security stakeholders are
5268 prepared with timely and appropriate threat information. IRM provides capabilities for
5269 stakeholders to collaborate and to facilitate integrated decision-making. Collaboration may occur
5270 for strategic or tactical intent. The countermeasures analysis and prioritization include a
5271 comprehensive mix of policies, procedures, technologies, and communications between
5272 stakeholders appropriate to the alternatives enumerated.

5273 The monitoring and analysis process is inherent in the five phases of risk management to not
5274 only evaluate the effectiveness but also refine IRM decisions continuously.

5275 2.2 SECURITY RISK MANAGEMENT

5276 The five phases of risk management mentioned above are applicable to the full spectrum of
5277 timeframes, ranging from strategic (years/months/days) to tactical (days/hours/real-time). Each
5278 phase must be integrated into each NextGen security layer. In this section, the strategic aspect
5279 related to each security layer is included. For the tactical aspect of each security layer that
5280 specifies how the IRM strategies are employed in a given domain, refer to the specific security
5281 layer IRM sections. The NextGen IRM capability enables the development of risk-based
5282 assessment strategies, vulnerability analyses, and complete compendiums of attack consequences
5283 related to threats for the NextGen. This capability also ensures the operational validity of the *risk*
5284 *profile of the flight object* and the *risk profile of the aviation facility*. These two profiles play a
5285 crucial role in governing how the NextGen Security system will implement its operational
5286 procedures in specific circumstances.

5287 **2.2.1 IRM—Secure People**

5288 The IRM—Secure People capability enables the development of risk-based assessment
5289 strategies, analyses of vulnerability, and estimation of attack consequences related to screening
5290 people at check-points, passengers, and aviation workers for the NextGen. One major function
5291 within the IRM—Secure People is to define the watch lists and factors that determine the relative
5292 risk ratings. Those airport workers with continued access would be required to undergo periodic
5293 (random) and regularly scheduled updates of their security and risk profile. Passengers and
5294 aviation workers are checked against these lists to assess their risk level. In addition, IRM—
5295 Secure People capability also identifies behaviors associated with high-risk people that airport
5296 security personnel could use in surveillance.

5297 Key to the selection of appropriate risk management strategy is the comprehensive analysis of
5298 threat event mitigation procedures. Often, this is accomplished through operational threat
5299 scenario analysis. For instance, countermeasures for a checkpoint breach scenario include an
5300 analysis of the range of effects and mitigation strategy for the mitigation of those effects.
5301 Although technology insertion is a vital part of the IRM—Secure People countermeasure
5302 strategy, it is important to regard the technology (or combination of technologies) as only one
5303 piece in the decision chain. Of equal importance to the technology selected is the promulgation
5304 of appropriate policies for the use of technology (e.g., carry-on baggage alarm resolution
5305 processes) and appropriate search strategies to be applied. Coupling various capabilities (e.g.,
5306 watch lists and behavior profiles) can maximize the threat detection capabilities of each, if
5307 carefully integrated.

5308 **2.2.2 IRM—Secure Airports**

5309 Security of NextGen Airports is central to preventing attacks against aircraft within the airport
5310 terminal area, either from local intrusion or attacks carried out on the ground, by intrusion onto
5311 the airport operations area (AoA), the public area, the sterile area, the remote facilities, or from
5312 the air. In addition to routine screening of passengers, bags, and cargo, airports also screen for
5313 threat all concessionaire materials for resale, goods, and liquids. Attack targets vary greatly:
5314 people, fuel farms, tower, operations centers, electrical infrastructure, and aircraft. Projectile or
5315 Man Portable Air Defense System (MANPADS) attacks from beyond the perimeter of the airport
5316 are also included in the individual airport's threat profile.

5317 The NextGen IRM—Secure Airports capability enables the determination of the risk profile of
5318 the aviation facility and the identification of the high-risk airports and related facilities that
5319 require additional security resources, technology investments, and more robust security
5320 operations to receive the appropriate levels of protection. The process also identifies airports that
5321 have low-risk profiles that do not mandate much if any security upgrade. Many criteria are used
5322 to determine risks, for example—

- 5323
- High-demand airports with large enplanements and international operations
 - Airports in designated high-risk geographic locations
 - Airports with special events/activities (e.g., frequent VIP presence).
- 5324
- 5325

5326 Each airport above a defined risk profile threshold performs a threat and vulnerability analysis
5327 that is updated periodically. The vulnerability analysis includes the entire physical footprint of
5328 the airport, out to the fence line and beyond to include the MANPADS threat. Each airport must
5329 develop and implement an airport security protection plan based on sound practice and pertinent
5330 airport security design.

5331 Assessments and priorities as to probabilities of attack follow from the five steps enumerated in
5332 Section 2.1. Such analyses indicate the most appropriate direction for the application of
5333 countermeasure and mitigation procedures and resources in the airports, including airport
5334 terminal building public area, at the screening checkpoints, inside the concourse sterile areas,²
5335 and on-the-air operations area. Passenger prescreening, passenger boarding physical screening,
5336 and carry-on baggage screening system capabilities respond to the risk profile and threat
5337 situation provided by IRM (e.g., higher alert state, special events, high risk airports) with various
5338 measures.

5339 Selected prioritization strategies to enhance the robustness of Airport security include an
5340 appropriate mix of people, procedures, infrastructure, and technology specific to the alternatives
5341 analyses and the countermeasures analyses. Similar to IRM—Secure People, technology
5342 investment is only one piece in the overall risk management of airports and is balanced with
5343 policy and procedures.

5344 **2.2.3 IRM—Secure Checked Baggage**

5345 The NextGen IRM—Secure Checked Baggage capability performs assessments and develops
5346 priorities as to probabilities of attack with various threat objects. Threat objects for checked
5347 baggage include explosives and improvised explosive devices (IED), CBRN materials, and other
5348 hazardous materials. Such analyses provide the most appropriate strategy for the application of
5349 countermeasure and mitigation procedures and resources. For example, as the Secure People
5350 capability identifies higher risk passengers, they should receive more stringent screening;
5351 however, there is a concomitant cost of resources and screening time depending on the criterion
5352 values for different levels of risk. The IRM Secure Checked Baggage process analyzes the
5353 various costs and benefits with the mitigation procedures to arrive at the best balance of threat
5354 reduction for the available resources and other constraints.

5355 Similar to the discussions in previous sections, using detection technology as a risk mitigation
5356 strategy is incomplete without considering policy, procedures, and other strategies. Technologies
5357 are useful only to the degree that they assist the human operator in decision-making. In addition,
5358 the “throughput” of the technology has a major impact on the processing rate of baggage and
5359 thus has impact on overall aviation commerce and system efficiency.

5360 **2.2.4 IRM—Secure Cargo/Mail**

5361 The NextGen IRM—The Secure Cargo/Mail capability process assesses risks for cargo/mail
5362 throughout the shipping chain from source to exit from the NextGen. The shipping chain
5363 includes cargo source, containerization, freight consolidation/forwarding, cargo/mail screening

² Secured areas are those that require positive identification with credentials (badge, smart card, etc) and controlled access.

5364 locations, air transport to destination, and all intermediate storage and transport. (The Cargo
5365 Source is defined as the entity in physical possession of the cargo immediately before transfer
5366 into an approved sterile area for assembly and packing or approved cargo screening system
5367 operation.)

5368 The risk assessment is based on the freight management system information supplied by the
5369 NextGen Secure Cargo/Mail capability. IRM—Secure Cargo/Mail can identify the risk level of
5370 given types of cargo (e.g., difficulty in screening) and the risk profile of the flight object and the
5371 aviation facility. Such analyses use many criteria to determine risks, for example:

- 5372 • Volume and types of cargo (e.g., break bulk, containers, commodities)
- 5373 • Operators (e.g., airlines, airports, shippers) cargo integrity procedures
- 5374 • Cargo geographic origin(s) and routes
- 5375 • Passenger flight or cargo flight
- 5376 • Size/weight of aircraft
- 5377 • Cargo operations' proximity to the traveling public at the airport.

5378 Threat objects for cargo and mail include explosives, CBRN materials, and other unapproved
5379 hazardous materials. The risk profiles determine appropriate detection capabilities and
5380 procedures for mitigating the risks of penetration and attack through cargo/mail. For example,
5381 screening for “live cargo” must be processed very differently from other cargo.

5382 For higher risk operators and operations, IRM—Secure Cargo/Mail develops strategies for
5383 specific mitigation measures. Depending on the risk type and level, such measures may include
5384 additional screening by shipper, airport, air carrier, or security service provider (SSP); detection
5385 technology deployment; extra placement of cargo security screeners; use of canine detection
5386 teams; and more frequent inspections of cargo operators and procedures for diverting some
5387 (slightly) higher risk cargo from passenger flights to ground transport. In addition, IRM—Secure
5388 Cargo/Mail coordinates with the Secure Airports (see Section 4) capability to develop
5389 appropriate airport requirements to mitigate cargo operations risks at airports (e.g., where to
5390 place cargo operations at a high-enplanement airport). IRM—Secure Cargo/Mail has integration
5391 requirements with the “Secure Aircraft” capability to develop appropriate measures for cargo
5392 protection on board the aircraft—container and cargo hold.

5393 **2.2.5 IRM—Secure Airspace**

5394 The NextGen IRM—Secure Airspace capability identifies locations of national critical
5395 infrastructure, assets, population centers, and activities (e.g., national sports events) that might
5396 warrant additional airspace protection. Using the locations identified, the IRM—Secure Airspace
5397 determines an airspace risk profile based on the IRM risk assessment process. These risk profiles
5398 guide flight planning, security restrictions, and response to anomalies/incidents. The risk
5399 assessment criteria include many variables like size and performance of aircraft, type of operator
5400 (e.g., general aviation, commercial passenger airline operations) domestic or international traffic
5401 and proximity or actual access to the airspace.

5402 The IRM—Secure Airspace process drives the development of risk-based access criteria that the
5403 Secure Airspace (Section 7) capability uses to set the integrated aircraft's security profile—for

5404 example, people and baggage prescreened (Secure People and Secure Checked Baggage
5405 capabilities), cargo prescreened (Secure Cargo capability), weight class of aircraft, and
5406 acceptable security factor (see Secure Aircraft, Section 8; Total Flight Monitoring concept
5407 described in Chapter 2 of the Concept of Operations Version 1.2). The IRM—Secure Airspace
5408 determines the risk likelihood of various types of operations. IRM also develops airspace access
5409 strategy for Secure Airspace (Section 7) to implement. For example, IRM can determine a
5410 certain weight class of aircraft poses lower risk (e.g., low end of general aviation [GA] aircraft or
5411 that unmanned aircraft system [UAS] operations above a certain weight size requires special
5412 restrictions).

5413 **2.2.6 IRM—Secure Aircraft**

5414 The NextGen IRM—Secure Aircraft capability assesses the likelihood of risks for various
5415 aircraft types. This would include risks to the aircraft itself, as well as the risk of the aircraft to
5416 be used as a terrorist instrument. Criteria used for determining the risk factor for aircraft include
5417 the following:

- 5418 • Aircraft size and weight
- 5419 • Amount of fuel on board
- 5420 • Passenger and or cargo flight
- 5421 • Number of passengers
- 5422 • Origin/destination/path/time of flight
- 5423 • Flight screening results—whether there are higher risk passengers or cargo on board
- 5424 • Presence of law enforcement officers (LEO) on board.

5425 Based on the risk assessment results, IRM—Secure Aircraft develops risk mitigation strategies
5426 that can deliver varied levels of security performances for the aircraft:

- 5427 • Install sensors on board, such as—
 - 5428 – CBRNE sensors in cargo hold
 - 5429 – Video monitoring in passenger cabin
 - 5430 – Continuous air monitoring
- 5431 • Harden aircraft frame or other structures
- 5432 • Deploy security personnel on board
- 5433 • Install MANPADS countermeasure technology or implement countermeasure procedures
- 5434 • Implement biometrics control for cockpit access
- 5435 • Implement special security procedures
- 5436 • Require high availability air-to-air and air-to-ground communication.

5437 The IRM—Secure Aircraft capability also develops risk envelopes for the NextGen security
5438 factor to be used by the total flight monitoring capability. This value is not meant to be simply a
5439 singular value; it could be a “profile” that depicts the “risk” aspect of a particular flight.

5440 Similar to discussions given in previous sections, it is important to balance the selection and use
5441 of technology (or combination of technologies) with policies, procedures, and economics impact.
5442 To the extent possible, safety-based aircraft modifications are leveraged for mitigation of
5443 security risks.

5444 **2.3 NEI-ENABLED INTEGRATED RISK MANAGEMENT COLLABORATION**
5445 **ENVIRONMENT**

5446 As discussed in previous sections, Security IRM uses the NextGen NEI capability to receive all
5447 applicable, authorized information within the NextGen as inputs to IRM’s risk assessment
5448 analysis and then to distribute outputs from the IRM process to all the authorized stakeholders as
5449 needed. In addition, the SSP-based IRM provides various analytical capabilities and information
5450 sharing environment to collaborate with the stakeholders, either in strategic timeframe
5451 (months/days/hours) or tactical timeframe (hours/minutes/real-time). Built on a NextGen NEI
5452 foundation, NextGen IRM makes use of a federated risk assessment collaboration infrastructure,
5453 which is provided by security stakeholders to perform, for example—

- 5454 • Collaboration and communication capabilities
- 5455 • Aviation system monitoring
- 5456 • Risk analysis tools
- 5457 • Risk scenario modeling capability suitable for the stakeholder mission
- 5458 • “What-if” and decision support capabilities to assess efficiency and effectiveness of risk
5459 mitigation strategies to support strategy development such as
 - 5460 – Investment portfolio (e.g., combination of technology)
 - 5461 – deployment/personnel/infrastructure to high risk airports)
 - 5462 – Technology insertion
 - 5463 – Adaptive security measures for security layers
 - 5464 – Resource and asset reallocation (e.g., allocation of baggage and cargo screeners and
 - 5465 – deployment of MANPADS countermeasures at airports)
 - 5466 – Technology tailoring (e.g., sensitivity and throughput of sensors)
 - 5467 – Procedure changes (e.g., screening and alarm resolution)
 - 5468 – Airspace restrictions
 - 5469 – Traffic flow changes
- 5470 • Security alert identification, reporting, and status determination and escalation.

5471 Because the NextGen security risk management stakeholder community is diverse and involves
5472 multiple government organizations that interact with their constituents and users, the NextGen
5473 IRM has a unified command, control, and communication (C3) framework for integrated risk
5474 management decision-making.

5475 This unified C3 has the following foundational aspects:

- 5476 • Clarity of roles and responsibilities of NextGen security stakeholder group for various
5477 aspects of IRM. The stakeholder group includes the SSP, defense service provider (DSP),
5478 air navigation service provider (ANSP), aviation system users, aviation transport, and
5479 airport authorities
- 5480 • An established set of standard operating procedures (SOP) that change to meet evolving
5481 threat
- 5482 • Well planned logistics for preparedness, response, and recovery
- 5483 • Robust training and joint exercises.

5484 This operational framework for the unified C3 enables the NextGen IRM stakeholder group to
5485 coordinate its decisions and actions in a timely manner across all aspects of performance.
5486 NextGen capabilities based on operational improvements in technology and procedures are
5487 seamlessly integrated with security processes to meet the needs of multiple areas (e.g., flight
5488 object security, ATM, airport facility security).

5489 **2.4 RISK MANAGEMENT STRATEGY MONITORING AND FOLLOW-UP**

5490 To assess how well the risk management process works and continue to refine NextGen risk
5491 strategies (mitigation and execution), the IRM process uses operational data to constantly update
5492 and refine its methods and outputs.

5493 NextGen IRM has a monitoring and follow-up capability that includes the following:

- 5494 • Data collection and analysis
- 5495 • Metrics analysis
- 5496 • Risk management modification process—for example,
 - 5497 – Changes of criteria and input parameters used in all the steps of the risk management
 - 5498 process
 - 5499 – Changes in risk scenarios (modified and/or new ones)
 - 5500 – Changes in security envelop threshold (e.g., for the security factor in the total flight
 - 5501 monitoring capability).
- 5502 • Identification of gaps and areas for improvements in, for example—
 - 5503 – Technology
 - 5504 – Infrastructure
 - 5505 – Process and procedures
 - 5506 – C3 roles and responsibilities
 - 5507 – New stakeholders.
- 5508 • Tracking of follow-up actions.

5509 Inherent in the process would be the supervision and analysis process for the five phases of the
5510 risk management process. A set of testing and evaluation procedures is institutionalized in
5511 sequence to evaluate the effectiveness of all five phases.

5512 **3 SECURE PEOPLE**

5513 No aspect of the NextGen security architecture is more important to the perception of a secure
5514 aviation system environment than publicly visible or implicit checkpoint and carry-on baggage
5515 screening operations. Other less visible security procedures may work similar ends and do so as
5516 effectively. However, the visible aspect of checkpoints and baggage screening is still most
5517 tangible and hence most relied on by the public in establishing its level of confidence and
5518 thereby its use of the system. The checkpoint displays an operating profile of consistency and
5519 routine, while behind the scenes, it has several new screening techniques and tools that can be
5520 leveraged for the assessed risk, and occasionally, performed randomly as an added measure.

5521 In the NextGen, the Secure People capability of the security architecture puts greater reliance on
5522 a more integrated approach correlating credentialing and identification processes with screening.
5523 Aviation security risks are mitigated by identifying and preventing people who, whether travelers
5524 or aviation workers, are a potential threat from gaining access to the air transport system through
5525 prescreening and credentialing, screening, and intervention. For travelers, aviation security is
5526 provided continuously from the time the reservation is made until the safe arrival of the flight at
5527 the final destination airport. For aviation workers, a standardized credentialing process and
5528 identification technologies prevent unauthorized individuals to access restricted areas of the
5529 airports. Those airport workers with continued access would be required to undergo periodic
5530 (random) and regularly scheduled updates of their security and risk profile. The NextGen Net
5531 Enabled Operations ([NEO]; the decision support and other applications using NEI for
5532 information transfer and retrieval) permits more valid and faster credential verification. A
5533 balance between security and customer service is maintained, permitting the consistent, efficient,
5534 and seamless movement of passengers at the airport.

5535 **3.1 INTEGRATED RISK MANAGEMENT**

5536 Continuous threat assessment and risk management processes identifies vulnerabilities and risks
5537 associated with people, whether travelers or aviation workers, moving within aviation facilities
5538 and the air transportation system. Mitigation strategies and countermeasures depend on
5539 threat/alert levels. Integrated decision increases decision quality and decrease response time to
5540 events. (See Section 2, Secure People.)

5541 **3.2 AUTHENTICATION AND CREDENTIALING**

5542 Authentication and credentialing processes are performed for passengers and the full range of
5543 aviation system employees, including airport, airline, vendors, maintenance and utilities, law
5544 enforcement, and government service providers (ANSP, SSP, DSP). Credentialing in this context
5545 is essentially the granting of a right of access while authentication is the verification of that right
5546 of access in a given situation or time. The positive identification of people is part of the layered,
5547 adaptive security system, which are based on levels of security, location, and net-centric
5548 information sharing. NEI operational linkages directly connect distributed users, enabling a more
5549 transparent and less interactive process and reduced transaction times. Biometric identity
5550 management ensures that passenger identities are preserved despite name and/or address
5551 changes, and mitigate the use of fraudulent credentials. All persons entering any virtual or
5552 physical secured area of the civil aviation system are automatically assessed and verified and,

5553 where appropriate, their identities are verified by NEI-linked biometrics. Biometric identification
5554 validation and authorization verification for this purpose is a key component to the screening
5555 system.

5556 **3.2.1 Credentialing**

5557 NextGen Aviation credentialing programs conduct background checks of aviation industry
5558 employees based on biographic and biometric information. Aviation workers include airport and
5559 airline employees, vendors, shippers, and service providers for the operations and maintenance
5560 and the service of aircraft, cargo, aviation facilities, and aviation infrastructure. The person's
5561 identity is authenticated on attributes permitting positive identification for access to secured
5562 areas (e.g., tarmac, aircraft, and cargo and baggage conveyances).

5563 Passenger credentialing programs permit passengers certain access rights or privileges that are
5564 unavailable to noncredentialed passengers. The credentialing process is conceptually similar to
5565 that performed with aviation system employees, although obviously the kinds of information
5566 needed to receive the credential vary.

5567 **3.2.2 Passenger Authentication**

5568 Prescreening is the process of checking passenger information against government watch list
5569 information or noting the absence of expected confirmatory data to the query to determine the
5570 risk status of that individual to enter the concourse sterile area³ of the airport and/or to board a
5571 commercial flight. The relatively lengthy period of time between reserving a flight and the actual
5572 departure date for the majority of passengers provides an opportunity to assess risk before
5573 individuals even arrive at the airport. However, the NEO capability allows 1-second verification
5574 so that on-demand passengers using an air taxi or very light jet (VLJ), with appropriate
5575 credentials, can be effectively verified before flight. Prescreening of individuals occurs every
5576 time a flight reservation is made. A flight reservation may include the itinerary of one or more
5577 individuals. All individuals on the reservation are prescreened before their arrival to the airport.

5578 The NextGen passenger prescreening leverages advances in information technology (IT) systems
5579 provide data sources and seamless information flow from passengers as they travel through the
5580 airport. Prescreening compares reservation information against known and validated threat and
5581 vulnerability information before local and/or remote check-in. Depending on prescreening
5582 results, a small percentage of individuals are required to further verify their identity. Even before
5583 a passenger checks-in at the airport or remote site, uplinked information could be made from
5584 his/her handheld devices to register identification information (e.g., biometrics, digital photo, or
5585 biographical data) to verify that the passenger is not a match to a government watch list or that
5586 verification information meets criteria.

5587 As part of the prescreening process, most individuals are able to travel expeditiously through the
5588 checkpoint and into the sterile areas. Those persons exceeding certain risk levels (without being
5589 identified as no-fly) receive enhanced screening at passenger security checkpoints in addition to
5590 more intensive checked baggage screening of any checked bags. The NextGen prescreening

³ A sterile area is one in which passengers have been through security checks.

5591 process includes a degree of randomness in occasional selection of individuals for secondary
5592 screening. Some airports may opt to allow passengers and nonpassengers through the security
5593 checkpoint. In this scenario, nonpassengers must have adequate credentialing.

5594 Consistent with civil liberties, identity verifications are performed locally or through net-enabled
5595 operations at each transaction such as when reservations are placed, before check-in, or when a
5596 person seeks to pass through an airport's access control point, to enter a sterile area or to board
5597 an aircraft. Privacy is maintained by advanced encryption and assembly of segmented data as a
5598 virtual temporary data object for authentication. Upon completion of the transaction, the data
5599 segmentation is restored with only a record log that an authentication event occurred. Derivative
5600 threat assessment values enable the activation of adaptive screening or other security systems,
5601 protocols or procedures. Some measures must apply to all threat levels, guarding against terrorist
5602 or criminal threats to the aviation system.

5603 **3.2.3 Aviation Industry Worker Authentication**

5604 The authentication programs also exist for aviation system employees (e.g., airport workers,
5605 airline employees, vendors, and LEOs) when they access various parts of the NextGen in
5606 performing their duties. The person's identity is authenticated on attributes permitting positive
5607 identification for access to sterile and or secured areas (i.e., those areas with access controls).
5608 Net-enabled operations linkage enables a more transparent and less interactive process and thus
5609 reducing transaction times, enabling 1-second identification on demand. All persons entering any
5610 virtual or physical aspect of the civil aviation system requiring credentials is automatically
5611 assessed, and where appropriate, their identities are verified by NextGen biometric information.
5612 This action applies at many locations, but notably at access points to secured areas of airports
5613 and at the checkpoints where persons (e.g., armed law enforcement officers) seek to pass into the
5614 sterile area. Biometric identification validation and authorization verification for this purpose is a
5615 key component to the screening system. On the positive side, the primary benefit of integrating
5616 the prescreening function with credentialing systems is to reduce the number of unknown
5617 travelers and to improve accuracy of prescreening results. The transportability of aviation worker
5618 credentials to other airports also is facilitated.

5619 Access controls and biometric verification systems are used to prevent unauthorized individuals
5620 from entering secured areas. Depending on enhanced security requirements of more tightly
5621 controlled areas (e.g., fuel farms, navigation systems, cockpit, tower, command center),
5622 individuals require multifactor authentication (i.e., use of multiple access control methods). One
5623 potential access control scheme for a particular class of workers is a combination of one or more
5624 biometrics, a password, and radio frequency (RFID) card. For example, a maintenance worker
5625 who needs access to sensitive surveillance equipment must authenticate with a biometric, time-
5626 sensitive, and variable personal identification number (PIN). However, even before arriving at
5627 the secure area, the worker would need to use his identification card, which includes RFID
5628 technology for uploading the timestamp and access point onto the secured area.

5629 **3.3 CHECKPOINT PERSON SCREENING**

5630 The NextGen Secure People capability also includes checkpoint screening of persons and carry-
5631 on baggage. Checkpoint person screening primarily involves travelers with flight reservations,

5632 but may include other credentialed or noncredentialed airport, airline personnel, crew member,
5633 or private individuals authorized to enter the sterile area of an airport. Through the NEO
5634 capability, passenger screening includes data from risk assessment, behavior analysis, and global
5635 exchange of traveler information.

5636 Passenger screening systems detect CBRNE and weapons, are relatively unobtrusive, and have
5637 lower “hassle factor.” The aviation people security screening system must be just visible enough
5638 to provide a level of deterrence, giving perpetrators pronounced uncertainty for a successful
5639 outcome of a planned malicious event. The addition of a small, random selection of individuals
5640 for enhanced (secondary) screening is evident for this reason.

5641 Screening consists of a combination of sensors for CBRNE and weapons detection. The
5642 biological sensors can also sense certain symptoms of active disease such as elevations of body
5643 temperature. The NextGen person screening systems have small footprints as a result of sensor
5644 fusion and can be easily scaled for different size airports’ physical space and throughput
5645 requirements. Because of the accuracy of these systems, passengers rarely experience unplanned
5646 additional screening or inquiries from security personnel. If a threat object is discovered, the
5647 screening equipment alerts NextGen NEO applications, which immediately correlate other
5648 current data concerning the individual (e.g., carry-on and checked bags in the system, flight
5649 reservation data, and credential and prescreening data) to determine whether other potential
5650 threats might remain in the system.

5651 **3.4 CHECK POINT BAGGAGE SCREENING**

5652 To permit maximum passenger convenience, the NextGen security system generally allows
5653 passengers some carry-on baggage, the main exception being in the highest condition of alert.
5654 Checkpoint baggage screening functions are as follows:

- 5655 • Carry-on baggage screening
- 5656 • Situation response procedures
- 5657 • Alarm resolution procedures
- 5658 • Threat object control procedures.

5659 In the NextGen, the checkpoint screening systems are system engineered with various sensors
5660 combined into “one box” by advances in sensor fusion. These detection units have modular
5661 components and easily replaceable “firmware”; therefore, they are able to be easily modified to
5662 detect the changing range of threats and servicing while simultaneously minimizing the
5663 checkpoint “footprint” and configuration requirements. Thus, they can be placed in various
5664 locations in the airport with minimal “fit” problems needing to be resolved. For high-capacity
5665 airports, appropriately equipped nearby areas are provided for the purposes of the discreet alarm
5666 resolution of passengers and/or their carry-on baggage. Checkpoint screening is as automated as
5667 possible in an effort to increase throughput and minimize the number of screeners needed. The
5668 checkpoint control procedures and access control technologies preclude people from entering the
5669 sterile area through the passenger exit lane bypassing the checkpoint screening function.

5670 The checkpoint has a central command center function linked to the airport Security Control
5671 Center (SCC) through NEO to handle the two-way information flow with the checkpoint, the

5672 airport, and other SSP operational centers. If a threat object is identified, the screening
5673 equipment, through NEI, immediately triggers the NEO security system to correlate other current
5674 data on the individual (e.g., person screening systems, checked baggage in the system, flight
5675 reservation data, and credential and prescreen data) to determine whether other threats might
5676 remain in the system.

5677 Checkpoint screening systems undergo certification approval in accordance with NextGen
5678 standards for checkpoint CBRNE and weapons detectors. The SSP approves checkpoints as
5679 complete units. The checkpoint concept includes detection capability for the amounts, types, and
5680 configurations of explosive threat types, weapons and chemical and biological agents through the
5681 use of chemical identification detection devices, and nuclear and radiological threat types.
5682 Sensors are oriented to permit the passenger to proceed through a short passageway, making
5683 his/her way through a series of sensors. An alarm shunts the passenger off to an alarm resolution
5684 area in the checkpoint. The passenger's carry-on baggage proceeds down a separate passage
5685 proceeding through a series of detection devices to detect the presence of carry-on baggage threat
5686 types. If an alarm occurs on the passenger or his carry-on baggage, both are reunited for a second
5687 level of screening procedures and interaction with the passenger to resolve the alarm. If the alarm
5688 cannot be resolved, additional procedures are employed, up to involving the use of LEOs.

5689 Through the NextGen Airport design process, physical space is allocated to the discrete
5690 resolution of bags and/or passengers that trigger alarms well outside the flow of cleared
5691 passengers and bags. The increased accuracy of detection sensors minimizes the frequency of
5692 this secondary screening response. In addition, the increased specificity of the alarm permits
5693 more focused resolution procedures and faster go/no-go decisions. If a threat object is identified,
5694 control procedures and technologies are readily available for using qualified law enforcement
5695 people to safely contain the object. Redundant NEI communications links to the airport security
5696 coordinator, law enforcement, air carriers, and airport SCC are provided.

5697 Checkpoint screening increasingly also occurs at remote locations from the NextGen terminal to
5698 handle the increasing passenger and baggage loads. (See Secure Airport Remote Terminal
5699 Screening Site [RTSS]) for facilities related to remote screening of passengers and their
5700 baggage.) Passengers and luggage undergo screening at these remote locations and board
5701 transportation bound for the airport's sterile boarding area. The remote screening facility and the
5702 allocated mode of surface transportation are part of the sterile area. Screening at these locations
5703 is identical to that at the airport.

5704 **3.5 CONTINUOUS SURVEILLANCE AT CHECKPOINT/ACCESS SITES**

5705 The continuous surveillance of people within the public areas of the airport is discussed in
5706 Secure Airports (Section 4). This section is restricted to surveillance systems and procedures at
5707 airport checkpoints and access and exit sites. Video analysis tools are able to automatically
5708 detect anomalies with bags and people. Video analytics may also be used to detect behavioral
5709 anomalies (behavior pattern recognition [BPR]) and/or undesirable events and to provide
5710 additional data for correlating with suspect carry-on and checked baggage or interactions with
5711 other people in the checkpoint or sterile areas (e.g., co-conspirators).

5712 Beyond the security checkpoint, continuous security surveillance occurs at the gates within the
5713 aircraft. Video analysis tools are integrated with passenger information systems to provide alerts
5714 for anomalous behaviors or events. For instance, the surveillance system can recognize in
5715 automated manner certain atypical behaviors associated with elevated risk (e.g., BPR).

5716 **3.6 GLOBAL HARMONIZATION**

5717 The NextGen is committed to the efficient and safe movement of all air travelers to ensure
5718 security while promoting national competitiveness. The SSP is intimately involved with
5719 international bodies to minimize inbound travel of possible terrorists by use of globally
5720 harmonized screening activities. The SSP specifically benefits from joint development and
5721 investment from the international community to promote unified objectives for layered, adaptive
5722 aviation security for passenger prescreening programs. The SSP aviation security programs
5723 address international requirements for all aspects of secure people capabilities and appropriate
5724 related airport and aircraft activities.

5725 **4 SECURE AIRPORTS**

5726 The NextGen Airport (see Chapter 3 of Concept of Operations Version 1.2) has an integrated
5727 facility security system scalable to differing capacity, access, and risk environments while
5728 maintaining the required NextGen standards. The Secure Airport CONOPS includes
5729 technological and procedural measures to protect against the dynamically evolving threat. This
5730 flexible security system leverages advanced network-centric capabilities inherent in the NextGen
5731 to minimize redundant credentialing and access controls while providing shared situational
5732 awareness when security incidents occur or credentialing concerns surface.

5733 The NextGen airport NEO seamlessly links sensors and data sources from access and screening
5734 checkpoints for passengers, visitors, employees and vehicles, perimeters, and critical facility
5735 infrastructure. The airport security technologies and adjustable procedures are nominally
5736 transparent to passengers and cargo, but difficult to exactly predict by those who intend harm. In
5737 addition, the NextGen airport has resident response and recovery programs enabled through local
5738 and regional memorandums of agreements (MOA) and supported by the US Government (USG).
5739 In this connection, the net-centric operations of the NextGen maintain real-time connectivity to
5740 other regional airport operators, law enforcement and USG intelligence and SSP operational
5741 entities. These tools enable quick ramp-up response operations to incidents of national
5742 significance, including CBRNE attacks on the airport or within the region. The emergency
5743 response has been appropriately gamed and rehearsed to ensure the responders are fully prepared
5744 for any contingency.

5745 The layered and overlapping security systems are in place at the following types of airport
5746 facilities:

- 5747 • Commercial (passenger/cargo) airports
- 5748 • RTSS facility
- 5749 • General (public and private) aviation airports
- 5750 • Commercial spaceports.

5751 They also are in place in the following areas within these facilities as appropriate:

- 5752 • **Airside:** Security identification display area (SIDA)/AoA, terminal perimeter, terminal
5753 airspace (security)
- 5754 • **Landside:** Terminal public and commercial roadways and parking lots, terminal entry
5755 and Departure, airline ticketing kiosk/counter, sterile area, international arrivals/customs,
5756 SCC, response and recovery operations

5757 **4.1 IRM—SECURE AIRPORT**

5758 IRM—Secure Airport prioritization strategies to enhance the robustness of airport security
5759 selected for implementation include an appropriate mix of people, procedures, infrastructure, and
5760 technology specific to the alternatives analyses and the countermeasures analyses. Similar to
5761 IRM—Secure People, technology investment is only one piece in the overall risk management of
5762 airports and is balanced with policy and procedures. (See Secure Airports, Section 2.2.)

5763 4.2 AIRPORT FACILITIES

5764 4.2.1 Commercial (Passenger/Cargo) Airports

5765 Similar to the commercial airports of 2006, the NextGen Commercial Airport has scheduled
5766 passenger and cargo operations. However, a greater range of aircraft types (e.g., vertical takeoff
5767 and landing [VTOL], VLJs, super wide body, and UAS platforms) can cooperate at the same
5768 airport. The NextGen airport facility security consists of layered defensive systems designed to
5769 capture threat information on passengers, baggage, cargo, aircraft, and alert appropriate response.
5770 In addition, the facility infrastructure is hardened to better protect the public and aviation system
5771 employees from CBRNE threat objects used externally or internally on the facility.

5772 4.2.2 Remote Terminal Security Screening

5773 To facilitate the flow of passengers, baggage, and cargo, the SSP, airport authorities, and third-
5774 party approved security partners operate remote or offsite terminal check-in, security screening,
5775 and bag-check and screening facilities. A majority of RTSS serve super-density airfields to
5776 mitigate passenger movement demand and position initial security screening as far away from
5777 the terminal operations area as possible. The RTSS facilities are continually monitored and meet
5778 applicable security standards, whether fixed or transportable. Secure transportation services for
5779 passengers, baggage, and cargo are provided between the RTSS and the airport-secured transfer
5780 area designated for those categories. The transportable RTSS can be deployed during stress
5781 periods of traffic demand (e.g., special events) or in response to a National Significant Security
5782 Event. The technologies used (CBRNE sensors and weapons detectors), which are operated by
5783 the airport owner, USG, or a third party, are fully compliant with existing security regulations
5784 and standards. To the degree practicable, all luggage other than carry-on will be processed at
5785 curbside or off airport so as to not enter the terminal portal with the passenger-owners. Checked
5786 baggage will be processed remotely to the terminal passenger area.

5787 Specialized RTSS are used to screen airline supplies destined for use on an aircraft for CBRNE
5788 threat. As described in the Secure Cargo and Secure People sections of this chapter there are also
5789 credentialing and secure custody chain requirements for these on-board supplies.

5790 4.2.3 General Aviation Airports

5791 GA airports in the NextGen can employ an SSP-approved security system scaled to the
5792 operational load and available infrastructure to achieve a lower facility risk profile. The security
5793 status and assessed risk of the GA airport is determined largely by the nature of the infrastructure
5794 present (including access controls), whether the airport is attended or unattended, and the type
5795 and quantity of aircraft operating there. Some GA facilities have a defined perimeter as with
5796 commercial airports; however, the level of sensor usage varies based on the size and type of
5797 aircraft operating at the airport and the proximity to high-risk metropolitan areas, sensitive
5798 restricted airspace or other special factors. GA airports that do not have an approved security
5799 system essentially operate as they did before the NextGen. Low-performance aircraft in the most
5800 cases are not significantly affected by higher facility risk profiles. However, higher performance
5801 aircraft or those aircraft capable of transporting a significant payload may experience an increase
5802 in their own flight object risk profile when they fly in more sensitive security areas.

5803 **4.2.4 Commercial Spaceports**

5804 The NextGen spaceport has security systems in place that have substantial overlap with other
5805 NextGen airports. However, some specialized features are required (e.g., access controls,
5806 credential verification, perimeter defense) as a result of the increased risk aspect of spacecraft
5807 systems, hazardous materials (fuel storage), and special launch and landing areas. The spaceport
5808 net-centric operations have secure access to the SSP and DSP, validating hypersonic aircraft
5809 clearances as they reenter the atmosphere to land at that facility.

5810 **4.3 AIRSIDE**

5811 **4.3.1 AOA/SIDA**

5812 NextGen Commercial Airports use various credential verification, access control, and
5813 surveillance systems to safeguard the aircraft, fuel farms, and other sensitive terminal airside
5814 areas, based on assessed risk and random measures. These include aircraft surface movement
5815 tracking, authorized vehicles-only screening, employee tracking, vehicle and employee access
5816 control (e.g., biometric readers and other advanced employee credential verification systems),
5817 unauthorized sector entry alerts based on credential status/level, vehicle and transportation
5818 worker tracking and identification, CCTV (daylight/infrared [IR]) on ramp areas adjacent to the
5819 airframe and occasionally airborne surveillance systems (i.e., UAS) to detect and track threats.
5820 The sensor and credential verification data are transmitted to the airport SCC (GA airports may
5821 have an NEI link to only a nearby SCC) as part of the airport net-centric operations, preanalyzed
5822 by NextGen decision support software applications and displayed in a usable form for incident
5823 response and interdiction. This capability is guided by a continual update of the employee status
5824 via NEO applications and the IRM, ensuring that any change in risk status is updated at the
5825 required latency. An important feature of this capability is the tracking of noncooperative targets
5826 (persons with no identification [ID]) that surreptitiously enter the AOA and alerting them of an
5827 appropriate law enforcement response via the SCC.

5828 **4.3.2 Terminal Perimeter**

5829 The NextGen airport perimeter is protected in various ways that may or may not include physical
5830 fencing. Depending on assessed risk and the practical and safety requirements of the airport site
5831 and surroundings, sensors, access control systems (ACS), closed-circuit television (CCTV),
5832 patrols, or other procedures with local LEO might be used. Where required or otherwise
5833 available, sensor arrays tied to existing ground surveillance radar can detect movement through
5834 the perimeter and alert (a) CCTV nearby to acquire the target and send unmanned ground
5835 vehicles (UGV) and/or (b) UAS systems to track and monitor the target until it is cleared or
5836 stopped. Adjacent stakeholders are intimately involved in maintenance of the perimeter,
5837 including fixed base operators (FBO) and air cargo operators. (Each operation offers distinct
5838 opportunities for unauthorized entry through its portals and shall be considered independently in
5839 this CONOPS.) Airport law enforcement manages and operates this system, with data fed
5840 directly into the airport SCC via the NextGen net-centric operations.

5841 4.3.3 Terminal Airspace Security

5842 Where indicated by risk assessment as essential, a set of new ground-based defense systems can
5843 be deployed to protect the terminal airspace. These systems' operations are guided by the
5844 available information from net-centric connectivity to ANSP (e.g., Automatic Dependent
5845 Surveillance-Broadcast (ADS-B), Communications, Navigation, and Surveillance [CNS]) and
5846 UAS. These UAS systems have very small (nanotechnology) airframes that can be simply and
5847 cost effectively deployed around the community surrounding the airport and programmed to
5848 detect and defeat potential MANPAD activity, airport perimeter breach, or other suspect activity.
5849 The data received from the UAS systems are transmitted NEO, assessed, and acted on in the
5850 SCC.

5851 4.4 LANDSIDE

5852 Airport-related infrastructure redesign or modifications are guided by the *Recommended Security*
5853 *Guidelines for Airport Planning, Design and Construction* as a baseline. NextGen terminal
5854 security operations and potentially airport-related infrastructure (e.g., check-in, security
5855 screening, and bag-check/screening) are extended to remote and/or portable offsite terminal sites
5856 to better distribute initial security screening workload and increase throughput. Airport
5857 roadways, parking lots, and approach corridors are better protected with standoff CBRNE
5858 detectors and vehicle identification and tracking where required by risk assessment. Sensors for
5859 trace and radiated CBRNE and for operational procedures monitor public access areas of the
5860 airport terminal and sensitive facilities. ACSs for persons and vehicles and facility surveillance
5861 networks with NEO integration provide security in airside and vendor supply areas. The airport
5862 SCC, co-located in the onsite airport operations center (AOC), enables the real-time update of
5863 threat information and monitoring of airport operations and supports dynamic adjustments
5864 security layers based on risk assessments and intelligence.

5865 4.4.1 Airport Public and Commercial Roadways and Parking Lots

5866 A continuing threat to the NextGen airport is the vehicle-borne improvised explosive device
5867 (VBIED) or unconventional weapons of mass destruction (WMD). This threat is addressed
5868 through sensor arrays, CCTV anomaly detection, operational procedures, and other systems to
5869 detect threat vehicles before they gain entry or proximity to critical infrastructure. The airport
5870 LEO can activate installed recessed roadway barriers to manage vehicle access routes. Improved
5871 BPR techniques and decision support systems are employed by law enforcement officers and
5872 other trained personnel to identify individuals who might warrant closer scrutiny and possible
5873 intervention. The sensor data feeds directly into an airport SCC (shared regionally and nationally
5874 under the NextGen NEO as events dictate), transmits directly to handheld devices carried by law
5875 enforcement, and automatically directs police to intercept threat vehicles. Portable blast
5876 containment devices and reinforced shrouds are easily placed around the threat vehicle and
5877 provide enhanced blast mitigation or contain a CBRN threat.

5878 4.4.2 Terminal Departures Curb

5879 The terminal curb, which is the first point of contact with the physical facility, is monitored
5880 through CCTV systems able to detect anomalies in passenger behavior, vehicle size and weight,

5881 and loiter time of vehicles. The security systems at the curb are similar to those described in the
5882 preceding section on public roadways, although the systems can be refined for closer proximity
5883 detection and mitigation. Sensor systems detect trace or radiated CBRNE from a standoff
5884 position and alert to potential threat. Sensors are managed and monitored by the airport or third-
5885 party, and airport law enforcement is responsible for policing the area and emergency response.

5886 **4.4.3 Terminal Entry Portal**

5887 The NextGen airport has terminal CBRNE sensors that are positioned within public access areas
5888 (curbside doors and entryways) to guard against threat devices entering the facility infrastructure.
5889 Air samples can be obtained to alert to CBRNE threats and provide preliminary location and
5890 identification information to response and recovery personnel through NEO. BPR continues to
5891 be employed by authorized personnel assisted by decision support tools to provide another layer
5892 of defense to public access areas.

5893 **4.4.4 Airline Ticketing Kiosk/Counter**

5894 Although a significant and increasing proportion of ticketing and baggage transfers are
5895 conducted at RTSS (off the airport property or on site, but not in the main terminal), this function
5896 is still present to some degree at the airport. The airport security systems and procedures used in
5897 public access areas also apply to the ticket kiosk or manned counter.

5898 **4.4.5 Security Checkpoint**

5899 Design of airport security checkpoints is integrated with overall terminal design to facilitate the
5900 flow of passengers and commerce. The checkpoint is integrated through the airport SCC to the
5901 NextGen NEO to enable more rapid and effective LEO response. The SSP uses the information
5902 to check for correlations with security incidents in other parts of the NextGen that may signal an
5903 unfolding security event. The security checkpoint exit lane in NextGen makes use of airport
5904 CCTV/person recognition systems that can acquire individuals proceeding the wrong way
5905 through an exit lane, visually lock onto the image, and track the perpetrator when nearing critical
5906 areas (e.g., gates, employee entrances).

5907 **4.4.6 Sterile Concourse**

5908 In the sterile areas of the concourse, facility sensors remain active to detect any threats, and LEO
5909 BPR are in place to capture CBRNE and conventional threats carried by passengers. CCTV
5910 systems transmit data to programs capable of detecting anomalies (BPR) in passenger behavior,
5911 and tracking passengers of interest, such as a passenger attempting to breach the checkpoint.
5912 These systems are linked to NEO communications systems at the airport and transmit
5913 information to law enforcement, guiding the response to enable the LEO to intercept the threat.

5914 **4.4.7 International Arrival/Customs**

5915 Airport security systems for sterile and public access areas are used. The security systems used
5916 by the US Customs Service, while technically outside NextGen, have been harmonized with the
5917 NextGen Airport security systems. This harmonization includes reducing incompatibilities and

5918 redundancies of screening systems and providing connections between US Customs operations
5919 and the NextGen through the Airport SCC and NextGen NEO.

5920 **4.4.8 Airport Concessions, Food, and Beverage Security**

5921 Supplies intended for use at the airport public areas rather than transport on aircraft are handled
5922 through verified shipper and known source programs described in Secure Cargo. CBRNE
5923 screening is conducted when justified by risk assessment and for supplies not following Secure
5924 Cargo and Secure People requirements for the vendor supplies and personnel. Supplies intended
5925 for use in the sterile area have to undergo the procedures specified in Secure Cargo (Section 6).

5926 **4.5 AIRPORT SECURITY CONTROL CENTER**

5927 The SCC is a facility operated by an airport operator that fuses all surveillance and data input
5928 associated with that airport. Principally operated by a combination of law enforcement and
5929 airport operations personnel, its staffing and infrastructure levels coincide with the size of the
5930 facility and operation. The ACC is the main connection point between the airport security system
5931 and the SSP and its security operations centers, as well as other SCCs as required. Note that this
5932 does not imply a single connection point to the airport because the NextGen NEO has built-in
5933 redundant pathways for information flows. (The airport's ability to detect, prevent, respond to
5934 terrorist attacks, and recover in a way that maintains continuity of operations depends heavily on
5935 the flow of surveillance, indicators and warnings (intelligence), and operational control
5936 messaging.) The SCC uses extensive and task specific data mining, predecision analysis and
5937 decision support software applications to reduce the amount of irrelevant information while
5938 increasing the quality of incidents requiring at least identification, if not outright response by
5939 airport, LEO, or SSP personnel. The SCC provides early warning to the airport operators,
5940 necessary telemetry data to guide response decisions, and accurate and timely information on
5941 incident aftermath to enable effective contingency response and continuity of operations.

5942 **4.6 EMERGENCY RESPONSE AND RECOVERY**

5943 Through command and control systems operated by NextGen SSP, DSP and NEO, and through
5944 better defined policies and MOA involving first responders owned by various organizations and
5945 governmental agencies, the airport can quickly respond to a terrorist attack, security breach,
5946 criminal act, or disaster at the facility with the goal of saving lives, mitigating property loss, and
5947 containing the threat. The plans are routinely exercised to address CBRNE events and the airport
5948 maintains necessary staff and equipment for the initial response. Regional emergency
5949 management agencies, through the SSP or other authorized organization, can train and equip
5950 their staff to effectively respond to CBRNE attacks.

5951 5 SECURE CHECKED BAGGAGE

5952 The objective of secure checked baggage is to prevent checked baggage from endangering
5953 aircraft, aviation facilities, or people and from being used as a threat vector for the transport of
5954 CBRNE. Policy, procedures, and IT are combined to create the most effective system to
5955 accurately differentiate threats from normal commerce. Checked baggage screening equipment
5956 and sensors, with multisensor capabilities, are linked through secured NEO to the SSP and to
5957 LEOs and first responders. Between transfer into the NextGen baggage handling system and
5958 transfer out, services exist to identify and track checked baggage with tracking devices and
5959 related technologies and maintain link to passengers and boarding status information.

5960 5.1 INTEGRATED RISK MANAGEMENT

5961 The checked baggage screening system's capabilities respond to the risk profile and threat
5962 situation that IRM provides (e.g., higher alert state, special events, high risk airports) with
5963 different measures—for example, airports could change screening procedures, modify the sensor
5964 detection threshold, increase and decrease of random secondary screening, and deploy more
5965 security screeners or other personnel. The strengths and weaknesses of the devices and
5966 technologies determine the role each plays in the overall civil aviation security explosives
5967 detection mission. Identifying these roles ensures that investment decisions are appropriately
5968 made. Some considerations in placing CBRNE detector systems are those that are purely
5969 technical in nature, such as performance against threat types, bag throughput rate, and
5970 automation problems. Some nontechnical considerations are procurement and operational costs,
5971 system installation practicalities, public acceptance, and reliability and maintainability. For
5972 example, a decision regarding the inappropriate use of coherent x-ray scattering devices for 100-
5973 percent screening of checked baggage because of bag throughput limitations should not cloud an
5974 investment decision to use that technology in other more specific and pertinent detection
5975 schemes.

5976 Airport threat classifications are reviewed periodically and changes in status call for detection
5977 equipment adjustments. Airport vulnerability analyses include CBRNE detector system
5978 deployment considerations consistent with the overall CBRNE detector system CONOPS,
5979 individually tailored to fit that particular airport's needs. For instance, consistent with
5980 vulnerability analyses, equipment combinations responding to individual airports' needs can be
5981 identified airport by airport and managed, kept in proper working order, and supported on that
5982 basis rather than on an airline-by-airline basis. Equipment would then be rearranged or departure
5983 gates changed, depending on daily protection needs. The process leads occasionally to
5984 considerable changes in airport passenger flow and resultant terminal designs. (See Chapter 3,
5985 Airport Operations of Concept of Operations Version 1.2)

5986 IRM-secure checked baggage also takes advantage of NEO to adjust baggage screening based on
5987 risk. Before a flight's departure (upon reservation submission), IRM-secure checked baggage
5988 receives passenger data to assess overall NextGen security risk profile and, in turn, uses the
5989 IRM's alerting capability to share this risk information with all stakeholders through NextGen
5990 NEO. The stakeholders can respond and adapt to varying threat situations. Passenger
5991 prescreening using the integrated watch list identifies those items of checked baggage requiring
5992 additional screening. (See Section 2, Secure Checked Baggage.)

5993 **5.2 CHECKED BAGGAGE SCREENING**

5994 The NextGen checked baggage screening process, although having a significant correspondence
5995 with the baggage screening process instituted immediately after the attacks on 9/11, has
5996 incorporated several innovations that permit greater adaptability and flexibility with an expanded
5997 range of threat detection: a) sensor fusion for the full range of CBRNE threats, b) footprint
5998 reduction, c) reconfigurable or integrated systems for easy deployment, and d) NEI connections
5999 providing complete integration with NextGen NEO.

6000 The basic process for checked baggage screening functions is as follows:

- 6001 • Checked baggage screening
- 6002 • Alarm resolution screening
- 6003 • Threat object control procedures.

6004 **5.2.1 Screening**

6005 All checked bags undergo screening before being loaded on the airplane. This concept is in effect
6006 at all domestic airports. This identical technique or a screening technique determined to be
6007 equivalent is required at all international last point of departure (LPD) airports for us air carriers.

6008 First-level (initial) baggage screening is designed to meet requirements defined by legal mandate
6009 to detect CBRNE threat amounts, types, and configurations. The need to integrate competing
6010 technologies arises from the complexity of the threat. CBRNE detectors can be deployed as one-
6011 box or multistage systems combination/integration devices depending on the site. A remotely
6012 based operator/analyst (with certain technical assistance from proximally located baggage
6013 handling and troubleshooting staff) analyzes machine nonresolvable alarms and expedites
6014 security response, passenger notification, or additional screening when required. Many routine
6015 decisions and alternate tests to screen suspect threats are performed by the installed hardware and
6016 software systems in automated manner. However, the screening system's effectiveness is
6017 ultimately determined by the human operators/analysts' ability to resolve expeditiously what has
6018 been detected by system components.

6019 Bags that are cleared for loading aboard the airplane are segregated by carrier and flight, held in
6020 a sterile secure holding area, and loaded aboard the airplane. (See Security Sensitive Information
6021 Annex for additional details.)

6022 **5.2.2 Alarm Resolution Screening**

6023 The resolution of "alarm" bags depends on the nature of the alarm, contextual information
6024 related to the alert level, flight risk status, the passenger, and other similar alarms concurrently
6025 occurring in the SSP baggage screening system. Obviously, differing implications for the various
6026 classes of threats-suspected nuclear and chemical/biological threat objects would require the
6027 most elaborate caution because of their capacity to contaminate significant areas of the facility
6028 and surroundings. Policies, procedures, and integrated technologies are in place to handle these
6029 various circumstances. RFID or equivalent tags are attached to each piece of checked luggage to
6030 facilitate tracking in the airport and on the airplane and substantiate ownership. Note that one

6031 benefit of sensor fusion is the opportunity to perform confirmatory tests on a suspected threat
6032 object. The confirmatory tests, which are by different kinds of sensors, have the inestimable
6033 value of providing an independent assessment of the initial alarm. If sensor fusion and technical
6034 advances permit, these overlapping tests can be performed concurrently. If not, then they can be
6035 sequential and contingency based. (See SSI Annex for additional details.)

6036 **5.2.3 Threat Object Disposal**

6037 Policies, procedures, and technologies are available for the containment and disposition of bags
6038 determined to contain threat objects or materials. Where appropriate, threat objects are
6039 deactivated or otherwise made inoperative or detonated by explosives defeat systems. As a result
6040 of increased accuracy and specificity of the detection systems, the effect on airport operations
6041 can be better calibrated to the event and threat. Through NEO, the NextGen has shared
6042 situational awareness for these events and can adapt more quickly and economically to them. For
6043 example, flights may be able to land at a different concourses rather than diverting to another
6044 airport. In other more serious circumstances, flights may divert to a close alternate airport and
6045 when the plane arrives, local transportation is already there to ferry passengers and baggage.

6046 **5.3 CHECKED BAGGAGE SCREENING INSTALLATIONS**

6047 The differing environments in which baggage screening takes place put constraints on the
6048 CBRNE detector systems. These constraints can be physical limitations or ergonomic and policy
6049 considerations. Physical limitations include the amount of available space or strength of the floor
6050 in the building in which the system is to be deployed. Ergonomic considerations include noise
6051 level, processing time of a passenger bag, baggage handling requirements, ease of maintenance,
6052 and safety and health hazards. Policy considerations include the total cost of the system,
6053 including maintenance and personnel training for operators and inspectors.

6054 However, the greater variety of detection equipment that can be deployed in the NextGen
6055 permits customized installations by airports' threat classifications. Those with high threat
6056 vulnerability profiles would receive different combinations of equipment from those with low-
6057 threat vulnerability profiles. Similarly, screening locations with specialized or intermittent
6058 baggage screening have correspondingly tailored CBRNE detector deployments.

6059 **5.3.1 In-Line Baggage Screening**

6060 The NextGen uses in-line baggage screening installation at airports with high levels of
6061 enplanements. This action greatly enhances throughput, even with super-density operations.
6062 Checked baggage undergoes screening in the airport's baggage makeup area for the in-line
6063 system. Checked baggage is delivered to the baggage makeup area from the check-in counter by
6064 an automated baggage transport conveyor system to one or more CBRNE detections systems.
6065 After screening, bags that trigger an alarm are subject to alarm-clearing procedures and
6066 technologies.

6067 **5.3.2 Nonintegrated and Standalone Baggage Screening**

6068 Non-inline CBRNE detection system installations occur in airports and other screening locations
6069 that lack high throughput demands or where inline systems installations are not feasible for other
6070 reasons. They are designed as rapid deployable units for low-capacity demand and temporary
6071 and intermittent screening locations, and they can be deployed preintegrated with other airport
6072 customer service functions. These systems have either an automated baggage loading and
6073 unloading interface or a manual interface that is ergonomically designed to minimize safety and
6074 health hazards. With these systems, procedures are in place to ensure the chain of custody of
6075 screened baggage to the aircraft.

6076 **5.3.3 Deployable Baggage Screening Operations**

6077 Remote screening of checked baggage also occurs at locations away from the airport terminal
6078 building to handle the increasing passenger and baggage loads. Passengers and luggage undergo
6079 screening at these remote locations, and board transportation bound for the sterile boarding area
6080 at the airport. The remote screening facility and the transportation media are part of the sterile
6081 area. Screening at these locations is identical to that at the airport.

6082 Occasionally, the baggage screening systems are an integrated part of a deployable airport
6083 infrastructure component. These deployable units service smaller capacity or intermittent service
6084 airports that do not have a business case for supporting a large-scale or permanent infrastructure
6085 to handle security functions and might also incorporate other airport customer services. (See
6086 Chapter 3, Airport Operations of Concept of Operations Version 1.2)

6087 **5.4 GLOBAL HARMONIZATION**

6088 The SSP is intimately involved with international aviation organizations to minimize inbound
6089 checked baggage containing unauthorized CBRNE through the use of globally harmonized
6090 screening activities. The SSP aviation security programs for screening checked baggage have
6091 sought maximum adherence to the required standards without mandating a particular technology
6092 or process to achieve that standard. Countries meeting these standards benefit from expedited
6093 processing of checked baggage by avoiding redundant screening operations. The SSP offers
6094 consultative services as well as excess equipment transfers to facilitate the adoption and
6095 maintenance of baggage screening requirements in foreign airports with direct flights to the
6096 NAS.

6097 **6 SECURE CARGO AND MAIL**

6098 Cargo represents a critical vulnerability that was addressed historically mainly through the
6099 deterrence value of background investigations, inspections, and paper trails required of shippers,
6100 both known and unknown. The NextGen vision for cargo security moves beyond that to also
6101 include freight vulnerability assessments (through the IRM process), identifying the risk level of
6102 cargo, use of sterile area cargo packing areas, cargo transit safety and integrity, and CBRNE
6103 screening for air cargo.

6104 Secure cargo/mail has the objectives to prevent not only checked cargo and mail from
6105 endangering aircraft, aviation facilities, or people but also the air cargo system from being used
6106 as a threat vector. These objectives are met using a combination of policy, procedures, and IT to
6107 accurately differentiate normal commerce from threats. Cargo and mail screening equipment and
6108 container sensors, with multisensor capabilities, are linked through secured NEO to the SSP SOC
6109 and other analysis centers.

6110 The security of cargo and mail begins at the point of initial packing (or when that is uncontrolled,
6111 initial screening) with either the manufacturer, freight consolidator, air carrier, or licensed US
6112 customs broker. The SSP integrates all information related to the flight, cargo, and aircrew to
6113 provide additional information and ensure security during transit, enabled through NEO. It
6114 includes the following concepts:

- 6115 • Vetting for secure supply chain entity (SSCE)
- 6116 • Vetting for certified supply chain entity (CSCE)
- 6117 • Security screening
- 6118 • Loading and storage security
- 6119 • Surface transportation security/tracking
- 6120 • Cradle to grave tracking/integrity.

6121 The air cargo supply chain has many potential organizations and personnel involved in the
6122 transport of any given piece of cargo: a source or shipper, freight forwarders, indirect air carriers,
6123 and other commercial and government personnel. Because of the many potential transfer points,
6124 cargo and mail security have to take into account the entire custody chain. A continuous risk and
6125 threat assessment must be conducted to identify risks to the supply chain; assess those risks; and
6126 apply measures, procedures, and policy to reduce those risks to an acceptable level. A secure
6127 supply chain encompasses the concept that cargo must be initially packed in a sterile area and
6128 conveyed through a secure chain or custody to the aircraft. If any deviance from this process
6129 occurs, all cargo intended for air transport whether on passenger flights or all-cargo operations
6130 must undergo CBRNE screening from either the SSP or a CSCE. After CBRNE screening, the
6131 integrity of the goods shipped must be maintained until the cargo exits the air transportation
6132 system. SSCE and CSCE are regularly inspected for compliance. All personnel with access to
6133 shipped goods must be properly screened and trained to ensure a secure shipping environment. In
6134 addition, all cargo items are subject to random inspection and CBRNE screening to maintain
6135 necessary variability and verification of the supply chain.

6136 **6.1 INTEGRATED RISK MANAGEMENT**

6137 Before a flight's departure, IRM-Secure Cargo capability receives cargo, shipping, and other
6138 threat data to assess overall NextGen security risk profile and, in turn, and alerts the stakeholders
6139 concerning potential risks (e.g., higher alert state, special events, high-risk airports, types of
6140 cargo). Such information sharing is through the NextGen NEO. The stakeholders can thus
6141 respond and adapt to varying threat situations by having improved situational awareness. The
6142 cargo screening system capabilities respond to the risk profile and threat situation that IRM
6143 provides with different measures; for example, airports could change screening procedures,
6144 modify the sensor detection threshold, increase and decrease random secondary screening, or
6145 deploy additional security screeners or other personnel. A freight assessment threat management
6146 system evaluates specific information about shippers (e.g., the environment at the shipment
6147 origin and the individual or personnel processing and packing it) and the goods they ship (e.g.,
6148 the physical and logistical difficulty of screening the items or the detectability of inserted threats)
6149 and assigns corresponding risk scores that determine screening methods and air transportation
6150 constraints.

6151 IRM uses NextGen-unified NEO capability to notify all relevant stakeholders through NEO so
6152 mitigation strategies can be coordinated and implemented, and relevant operational data can be
6153 fed back to IRM—Secure Cargo. (See Section 2, Secure Cargo/Mail.)

6154 **6.2 SHIPPER CREDENTIALING**

6155 The NextGen security system for air cargo, with risk profiles rated in excess of a defined
6156 threshold, uses a tiered certification process offering certifications for SSCE and CSCE status
6157 based on various levels of screening capability, cargo integrity technologies, and other NextGen
6158 credentialing processes. (Note that the risk profile mentioned here is for the cargo item itself, not
6159 the flight object. See para D.6.3 for flight object risk and cargo.) Applications to join the SSCE
6160 and CSCE programs are vetted against terrorist and law enforcement databases. When assessing
6161 an application to join the SSCE or CSCE program, the SSP evaluates the character, reliability,
6162 and susceptibility to compromise the persons involved. Airlines operating under an all cargo
6163 security programs should accept cargo from only a shipper with an SSP-approved security
6164 program unless they have their own cargo screening operations.

6165 The Secure Supply Chain Entity Management System integrates shipper credentialing and
6166 regulated shipper-controlled security inspection processes to reach cargo security compliance
6167 targets while minimizing impact on commerce. The SSCE is responsible for enforcement of all
6168 regulations in the segments of cargo preparation, transport, and receipt it directly controls within
6169 a trusted and monitored chain of custody. Essentially, they must maintain and control a sterile
6170 environment for initial cargo item packing in accordance with approved specifications and
6171 configurations coupled with the direct (nonpaper based) verification of the containerization (e.g.,
6172 video records). Conveyance to the aircraft must be successfully completed through an approved
6173 SSCE or the cargo are subjected to CBRNE screening, unpacking or rejected for air transport.
6174 CSCEs also have the verified capability to perform nonintrusive technology-based CBRNE
6175 screening for some or all of their cargo shipment to expedite handling.

6176 **6.3 SCREENING AND INSPECTION**

6177 All air cargo associated with flight object risk profiles above a defined threshold and not meeting
6178 SSCE sterile area packing and chain of custody requirements are screened for CBRNE threats
6179 (mainly through specialized screening systems) before loading on an aircraft. Cargo screening
6180 can be conducted as early in the supply chain as a secure method of conveying it to the aircraft
6181 can be maintained. Cargo screening equipment typically accommodates standardized industry
6182 practices related to the movement of goods. The NextGen cargo screening process permits
6183 airport and offsite cargo screening facilities by CSCEs to ensure the free flow of commerce. If
6184 screened off site, the secure cargo supply chain ensures the integrity of the screened goods
6185 during transport to the air carrier. All persons who receive, inspect, transport, or load air cargo,
6186 or who have unescorted access to air cargo or all cargo aircraft have been vetted using relevant
6187 data bases or credentialed, as appropriate.

6188 To detect CBRNE agents and other threat materials, NextGen cargo security uses sensor
6189 technologies designed specifically for inspection of cargo intended for air transport by Direct Air
6190 Carriers. These systems deliver improved performance in throughput, threat detection,
6191 maintainability, ease of installation, and reduced false positives. A small proportion of cargo
6192 intended for air transport may not be capable of being screened effectively for all threats even
6193 with NextGen technology. These would need to be packed in accordance with SSCE sterile area
6194 requirements for cargo packing. Other procedures must be used in such circumstances through
6195 the SSCE and CSCE programs. For example, a CSCE source would verify a container's contents
6196 through a video record of the initial packing and, where required, with their own screening of the
6197 individual unpacked items. The package would be placed in a tamper-proof container and
6198 transported through secure ground transportation to the airport. An alternate approach would be
6199 to use an acceptable form of IED Defeat Technology to achieve the 100-percent inspection
6200 requirement.

6201 For the most part, pre-NextGen acceptance sites remain operational if useful, provided that cargo
6202 integrity can be maintained. However, NextGen has additional acceptance and cargo screening
6203 sites to improve the flow of commerce.

6204 **6.4 ALARM RESOLUTION**

6205 The resolution of "alarm" cargo containers depends on the nature of the alarm, contextual
6206 information related to the alert level, the shipper/source, and other similar alarms concurrently
6207 occurring in the SSP baggage screening system. Many of the same considerations apply as with
6208 checked baggage (see Section 5.2). The major differences are the relative inaccessibility of the
6209 shipper compared with the passenger and the general difficulty in opening cargo containers for
6210 inspection. Therefore, not every piece of intended air cargo is loaded onto an aircraft, although a
6211 vast majority do. For cargo items known to be difficult to screen, it is incumbent on shippers
6212 requiring air transport to adopt other approved means to verify their cargo, as in the example
6213 above. (See SSI Annex for additional details.)

6214 **6.5 SURFACE TRANSPORTATION SECURITY OF SCREENED CARGO**

6215 Cargo screened before arrival at the air cargo facility on airport is surrounded by a “chain of
6216 custody” umbrella providing NEO-linked tracking and protection, from origin (i.e., initial
6217 screening point) to the airport in a secure environment (e.g., truck), which is sealed and tamper-
6218 proof. Cleared unit load devices (ULD) are locked with tamper-proof seals and devices. Access
6219 controls for persons and vehicles are implemented on all cargo ramps that are the same or
6220 equivalent to SIDA requirements. (See Section 3, Secure People, and 4, Secure Airports.) All
6221 persons who screen, transport (after screening), load cargo onto the aircraft, or who have
6222 unescorted access to air cargo or all cargo aircraft, have credentials and receive authentication at
6223 access points.

6224 **6.6 HARDENED DOORS AND BARRIERS ON ALL CARGO AIRCRAFT**

6225 NextGen air cargo airliners have a special barrier between the cockpit and cargo areas to prevent
6226 persons in the cargo area from attacking the crew unawares. The barrier is sufficient to give the
6227 crew time to take necessary actions in response to the threat and signal the emergency. (See
6228 Section 8, Secure Aircraft.)

6229 **6.7 SECURITY TRAINING FOR ALL CARGO FLIGHT CREW AND STAFF**

6230 All cargo flight crews receive the same security training as passenger flight crews. This training
6231 includes Crew Member Self-Defense Program, Federal Flight Deck Officer training and BPR
6232 training, and access to pertinent SSP Security Directives and Information Circulars (see
6233 Section 8, Secure Aircraft). This also includes training in recognizing cargo that may have been
6234 tampered with.

6235 **6.8 STORAGE SECURITY**

6236 Once the cargo has been screened and cleared for shipment, the cargo remains in a sterile
6237 isolation, secured and protected until it reaches the aircraft cargo hold (at origination and staging
6238 areas on airport). These measures include physical security and application of technology to
6239 produce virtual barriers around the sterile area, capable of alerting any unauthorized entry.

6240 **6.9 CARGO TRACKING AND INTEGRITY**

6241 Throughout the transport process, the air cargo is tracked and monitored until it reaches its
6242 destination, again using NEO capabilities. Cargo is placed in containers with sensors/devices,
6243 which provide proof of tampering. For those cargo items or shipments identified by risk
6244 management as security risks if stolen/diverted, tracking, diversion, or other identification data is
6245 provided through NEO to the SSP.

6246 **6.10 GLOBAL HARMONIZATION**

6247 The SSP is intimately involved with international aviation organizations to prevent the shipping
6248 of unauthorized CBRNE materials to the United States through aircraft. The SSP aviation
6249 security programs for cargo tracking, screening, integrity, and screening have sought maximum

6250 adherence to required standards without mandating a particular technology or process to achieve
6251 that standard. Countries that meet these standards benefit from expedited processing of cargo by
6252 avoiding redundant screening operations. The SSP offers consultative services and excess
6253 equipment transfers to facilitate the adoption and maintenance of cargo-screening requirements
6254 in foreign airports with direct flights to the NAS.

6255 **7 SECURE AIRSPACE**

6256 The major objective for secure airspace is to prevent or counter external attacks on aircraft and
6257 other airborne vehicles anywhere in the NAS or to use an aircraft as a weapon to attack assets
6258 and events on the ground. To reduce the security risk within the Air Domain, NextGen Secure
6259 Airspace systems and procedures detect and prevent or mitigate: a) anomalies in aircraft
6260 operation that indicate unauthorized use or attempted unauthorized use, b) aircraft not providing
6261 the appropriate cooperative data concerning identity and intentions, c) external attacks on
6262 aircraft, d) aircraft that can pose a threat from operating in the NAS. These risk management
6263 requirements include defining (usually dynamically) the boundaries of security-restricted
6264 airspace (SRA) and temporary flight restrictions (TFR), the cooperative division of
6265 responsibilities between the DSP and the SSP in the event of security events in flight or by
6266 airborne threat aircraft, security personnel on flights, and modifications and equipment to the
6267 aircraft. SRA and TFRs will be implemented as a last resort throughout the NextGen network,
6268 not as a routine procedure. In addition, secure airspace implements airspace access and flight
6269 procedures based on a verification process that dynamically adjusts for aircraft performance
6270 capabilities. The model combines credentialing data with performance data as part of developing
6271 the risk profile of the flight object. One objective is to permit increased NAS access by low-
6272 performance aircraft through most restricted zones because the reaction time to intercept is
6273 correspondingly greater than with high-performance aircraft.

6274 **7.1 INTEGRATED RISK MANAGEMENT**

6275 The IRM—Secure Airspace process (see Section 7.1) identifies locations of security interest and
6276 establishes the requirements for NAS protection from the four threats described above in
6277 Section 6. This risk management process requires close coordination between the ANSP and SSP
6278 and in some areas with the DSP. For example, the SSP uses the intelligence and threat
6279 information made available in the IRM process (see Section 5.1) to establish the operational
6280 requirements for the SRAs, time interval, size of airspace, and access criteria. Through
6281 collaboration with the ANSP and the DSP, the access criteria incorporate the criticality of the
6282 protected site or object, the aircraft performance specifications, and the verification level
6283 (credentials) of an operator crew, passengers, cargo) to determine the SRA size for a given flight
6284 object. For flight objects governed by flight plans, the ANSP can use the risk profile to formulate
6285 an appropriate four-dimensional trajectory (4DT). Consequently, lower risk flight objects in the
6286 NextGen experience fewer restrictions through SRAs. Even low-risk flights operating on visual
6287 flight rules (VFR) (such as low-performance aircraft) have increased access through the
6288 dynamically defined SRAs.

6289 **7.2 VERIFIED AIRSPACE ACCESS**

6290 Integrated airspace operations (see Section 7.1) provides a full discussion of the types of
6291 airspaces in NextGen ranging from those with general or universal access to highly restricted
6292 zones attributed to performance requirements or security considerations. As noted, the NextGen
6293 ATM service received by a flight depends on the aircraft's performance and equipment
6294 capabilities and its flight object risk profile. From the security perspective, the right to transit
6295 through non-universal access NextGen airspaces is based on a verification process that brings

6296 together relevant information for defining a flight object risk factor. Aircraft unverified on one or
6297 more of the following risk factors is still able to operate in appropriate low-risk NextGen
6298 environments, but the lack of verification does affect their risk profile if they transit more
6299 restricted airspace. This method has the following summative verification and credentialing
6300 factors:

- 6301 • Flight operator’s security performance is certified based on SSP-issued requirements.
- 6302 • Aircraft is registered, and its legacy has chain of custody integrity.
- 6303 • Aircraft operator’s identity is known and verified before flight becomes airborne.
- 6304 • Crew and passengers have been credentialed before a flight becomes airborne (secure
6305 people capability).
- 6306 • Aircraft content (e.g., baggage/cargo/mail) has been screened (secure checked baggage
6307 and secure cargo/mail capabilities).
- 6308 • The aircraft has communication capability air to air and air to ground throughout flight to
6309 maintain verification status of identity and intentions.

6310 In the NextGen, verified aircraft have access to the full set of authorized functions for their
6311 equipage. This does not mean that all aircraft must satisfy all aforementioned security
6312 requirements to have access to the NAS. As discussed in Chapter 2 of the Concept of Operations
6313 Version 1.2 document, standard VFR operations can still be conducted in specified airspaces. In
6314 addition, low risk-profile flight objects operating with VFR often may have an increased level of
6315 access though security zones compared with pre-NextGen NAS procedures.

6316 **7.3 SECURITY RESTRICTED AIRSPACES**

6317 SRA airspace is put in place to protect key assets and activities that are of national security
6318 significance. Their geometry, volume, and activation schedules are efficiently structured and
6319 implemented to balance security and air traffic demand. The use of SRAs for security purposes is
6320 kept to the minimum required to maintain security standards and maintains as much flexibility as
6321 possible to avoid impeding the flow of commerce. In addition, NextGen SRAs are no longer
6322 defined in terms of distance units but instead as time-based units (i.e., time to transit or reaction
6323 time to intercept). An SRA is segmented into the SRA minimum zone in which transiting aircraft
6324 are not permitted and one or more risk-level extension zones. Higher risk profile aircraft have to
6325 avoid the maximum SRA zone while those with lower risk profiles can cross closer to the SRA
6326 minimum.

6327 If IRM—Secure Airspace identifies SRAs as a risk mitigation strategy to protect certain critical
6328 assets, locations, or activities, the NextGen secure airspace capability defines multiple
6329 alternatives for restricted airspace volumes and timeframes. This assessment leverages NextGen
6330 trajectory-based operations (TBO) capability to assess overall NAS impact based on projected
6331 demands. The “what-if” capability from TBO forms the analytic basis for determining the
6332 optimal SRA volume size, SRA minimum zone and extension zones, access criteria, and their
6333 associated security requirements and procedures.

6334 In the NextGen, it is envisioned that the temporally defined SRAs have the following general
6335 types:

- 6336 • Total restriction SRA (few locations)
 - 6337 – Airspace access is limited to only security and defense operations.
 - 6338 – No exemptions.
- 6339 • Continuous restriction SRA
 - 6340 – Airspace that has some security performance requirements to gain access.
 - 6341 – Access exemptions are risk based.
- 6342 • Intermittent restriction SRA
 - 6343 – Airspace that has high-security performance requirements for certain time periods;
6344 the remainder of the time, no restrictions.
 - 6345 – Access exemptions are risk based.

6346
6347 As noted, an SRA is based on the criticality of the protected site/object and the risk profile of the
6348 flight object and can be either permanent (e.g., the US Capitol) or short-term (e.g., nuclear
6349 materials transport at a power plant) for total restriction SRA. Continuous, but not total,
6350 restrictions SRA could apply to large metro areas that are major population centers. Intermittent
6351 restriction SRAs could apply to major sports or political events or locations that have large
6352 gathering of people for a limited timeframe. An exemptions process is available to handle special
6353 circumstance such as emergencies and activities that warrant special considerations (e.g., flights
6354 carrying foreign dignitaries). In addition, access to SRAs during severe weather conditions could
6355 also be a basis for exemption. The exemption process is conducted efficiently without incurring
6356 delay.

6357 **7.4 AIRSPACE VIOLATION DETECTION, ALERTING, AND MONITORING**

6358 The total flight monitoring capability in secure aircraft (see Section 8) calculates a security factor
6359 that is continuously being updated. In real time, the secure airspace capability receives data
6360 updating each flight's security factor. The separation management (SM) capability (Section
6361 2.2.8) detects potential violations of SRAs from cooperative and non-cooperative flights within a
6362 look-ahead time. The detected airspace violation alert notifications are sent to operational
6363 personnel who have positive control responsibilities for the aircraft, including the flight operator
6364 and ANSP. Depending on aircraft type, the cockpit may also be equipped with airspace violation
6365 detection capabilities that could alert the flight operator directly.

6366 The TSM automation proposes resolutions (e.g., reroute) to deconflict the airspace violations and
6367 the flight operator execute the resolution. Airspace violations are continuously monitored to
6368 ensure deconflict maneuvers are implemented. Alert status is escalated when the aircraft does not
6369 respond timely or take directed action to achieve authorized trajectories. If an airspace violation
6370 alert is not resolved in a timely manner, the NextGen SSP and DSP are notified. In addition to
6371 airspace violations, alerts concerning flight anomalies or behavior on board could be detected by
6372 the Federal Air Marshals Service (FAM), crew, or other LEOs and could potentially be reported
6373 through the following paths: FAMs/SSP and flight operator/ANSP. Such alerts are shared
6374 through the NextGen NEO with the DSP and other stakeholders.

6375 The alert situation is continuously monitored by automation and by the ANSP and SSP personnel
6376 to determine when/whether the alert status has to be further escalated. The secure airspace has a
6377 set of criteria for alert escalation, for example,

- 6378 • The same aircraft violates the restricted airspace multiple times.
- 6379 • An aircraft does not change its flight profile to avoid or exit the unauthorized trajectory
6380 or airspace.
- 6381 • An aircraft with an airspace violation has a security factor that exceeds the security
6382 threshold.
- 6383 • Multiple unauthorized aircraft penetrate the same airspace simultaneously.
- 6384 • Look-ahead time to point of (critical) violation is short.
- 6385 • The aircraft fails to communicate with the ANSP repeatedly.
- 6386 • Aberrant behavior on board is not resolved.

6387 The secure airspace capability also does automated recordkeeping of violations of SRAs. Such
6388 data are used for pursuing follow-through actions for noncompliant aircraft operators.

6389 **7.5 INTEGRATED MANAGEMENT OF AIRSPACE SECURITY**

6390 Response to airspace security incidents is time critical with many organizations that have to act
6391 simultaneously and/or sequentially. This response cycle of the incident management process is
6392 human-centered with automation providing information updates, situation monitoring, and
6393 decision support. NextGen IRM's unified C3 capability (see Section 2.3) provides the
6394 operational and communication infrastructure for notifying and facilitating collaboration with all
6395 relevant stakeholders, especially the ANSP/SSP/DSP, flight operator, and the flight operations
6396 center (FOC) through NEI so risk mitigation strategies can be developed, coordinated, and
6397 implemented. Through policy and standards development, NextGen has an integrated
6398 multiagency command structure with clear roles and responsibilities for decision-making, with
6399 one organizational entity at the lead position.

6400 **7.5.1 Non-Cooperative Surveillance**

6401 In the NextGen, all aircraft above a certain size or flying in specified environments must
6402 broadcast identifying information and respond to pre-designated queries. (All UASs without
6403 exception must do the same.) However, to preclude threat or other rogue aircraft from operating
6404 unannounced or surreptitiously in the NAS, the NextGen has a non-cooperative surveillance
6405 capability. (See Chapter 5, Non-Cooperative Surveillance of Concept of Operations Version 1.2)

6406 Upon detection of a non-cooperative aircraft, the SSP requests, through the ANSP, information
6407 on the flight. If the non-cooperative aircraft is not identified and cleared, the SSP initiates an
6408 alert to the appropriate SOC. Additional observation and data collection are initiated, which in
6409 critical circumstances may lead to DSP interdiction.

6410 **7.5.2 Countermeasures**

6411 When an alert reaches a high-severity level, the alert becomes an incident that the SSP and
6412 ANSP have to develop counter measures to reduce the risk. There are two countermeasure

6413 alternatives: reroute/diversion and/or interdiction. Reroute/diversion strategies are developed
6414 with considerations of minimizing impact on other flights and on the overall NextGen system.
6415 When an incident occurs, the unified command center leads the coordination and monitoring of
6416 the development of the incident. The ANSP is the direct interface with the flight. Consequently,
6417 while the incident is still being monitored and has not exceeded a risk threshold, the ANSP acts
6418 as the lead who consults with the SSP and DSP.

6419 Interdiction is another countermeasure option. This option could be combined with
6420 reroute/diversion. The interdiction countermeasure is used in situations, especially when an
6421 aircraft fails repeatedly to communicate with the ANSP. The ANSP, in close coordination with
6422 the SSP, makes the decision to interdict and seeks military assistance from the DSP.

6423 The DSP is responsible for providing the defense asset for interdiction. During interdiction, the
6424 defense provider continues to monitor the situation and coordinates decisions and actions with
6425 the NextGen combined operating command center. The DSP is in the lead during interdiction. It
6426 has a stringent set of engagement rules to ensure satisfactory interdiction outcome.

6427 **7.5.3 Joint Exercises**

6428 Response to airspace security violations involves many stakeholders; therefore, NextGen has an
6429 infrastructure and a set of simulation and training capabilities that could facilitate joint exercises
6430 (war-gaming) among many stakeholders. Such an infrastructure delivers “virtual” violation
6431 events as part of security scenarios to validate the plan and procedures put in place for security
6432 violations coordination, monitoring, and countermeasure execution.

6433 **7.6 COUNTER PROJECTILES**

6434 Projectiles, including MANPADS systems, are defined in the broadest sense here as any ground-
6435 launched projectile capable of bringing down an aircraft at altitudes from liftoff to 10,000 feet,
6436 including MANPADS, rocket-propelled grenades, anti-armor weapons, mortars, and other
6437 similar devices.

6438 **7.6.1 Airport AOA/Terminal Airspace**

6439 Local and regional intelligence is considered in the IRM assessments of MANPADS attacks to
6440 determine rank-ordering, prioritization, and otherwise assess the MANPADS threat at airports.
6441 The analysis includes a site-specific analysis of MANPADS threat corridors adjacent to the
6442 airport, airport perimeter security, counter MANPADS systems in place, and joint operating
6443 procedures established with local and adjacent LEO jurisdictions and with the SSP, DSP, ANSP,
6444 and Department of Justice (DOJ). The product of this continually updated process is a priority of
6445 mainly ground-based counter MANPADS installation investments at vulnerable airports but with
6446 some aerial surveillance by UAS and other aircraft. The aerial surveillance is concentrated on
6447 vulnerable terminal airspace based on threat. This process has policy implications because these
6448 systems (e.g., UAS, UGV, other NextGen sensor systems) are costly and may not necessarily
6449 enable rapid installation. The assessment also directs local LEO jurisdictions to develop and
6450 implement operational programs that provide added surveillance and interdiction capability on
6451 the ground. This preflight phase addressing counter MANPADS terminal operations is conducted

6452 well before a particular flight. Infrastructure or other system installations extend the lead-time for
6453 this phase.

6454 **7.6.2 Aircraft/Flight Object**

6455 Once a flight is planned, scheduled, or initiated, the IRM determined risk level is established for
6456 that flight or aircraft. The IRM information is tied to a flight object and continually updated with
6457 information obtained from the NextGen NEO until the flight concludes. Information relating to
6458 local or regional MANPADS threats can be assessed immediately via SSA links to local joint
6459 terrorist task forces (JTTF) and other LEO organizations. A threat spike of predetermined
6460 magnitude may direct the ANSP to affect a change in trajectory management (routing) or divert
6461 the flight object.
6462

6463 **8 SECURE AIRCRAFT**

6464 Secure aircraft increases the safety and security of the NextGen aircraft in flight through various
6465 hardware, software, personnel, and procedural methods. The threats that require mitigation are
6466 hijacking and unauthorized diversion, internal explosive destruction, external attack, onboard
6467 CBRN or other attack of crew, passengers, or aircraft systems, aircraft use as a transport for
6468 CBNRE, and aircraft use as a WMD. Secure aircraft applies to civilian passenger aircraft and
6469 civilian cargo aircraft. UAS aircraft (surveillance or cargo) also is included for threats related to
6470 unauthorized diversion, internal explosive destruction, and as a transport for CBRNE.

6471 **8.1 INTEGRATED RISK MANAGEMENT**

6472 Continuous threat assessment and risk management processes identify all security-related
6473 vulnerabilities and risks associated with various types of aircraft and aircraft operations and
6474 scheduling in the air transportation system. Mitigation strategies and countermeasures for a given
6475 aircraft depend on risk assessment and threat/alert levels. Integrated decision-making through
6476 NEO increases decision quality and decrease response time to events.

6477 **8.2 AUTHORIZED CONTROL OF THE AIRCRAFT**

6478 Maintaining authorized control of the aircraft is the most essential and obvious step to preventing
6479 using aircraft as a WMD and to other hijacking/unauthorized diversions. (Note that the aircraft
6480 may either have a pilot/crew or be a UAS.) However, it also prevents or significantly mitigates
6481 the threat of aircraft cabin.

6482 **8.2.1 Cockpit Systems**

6483 The NextGen aircraft assessed to be a significant risk for use as a WMD or hijacking diversion
6484 has certain aircraft hardware and software systems that the pilot or UAS controller can use to
6485 prevent unauthorized diversion or, at the least, provide a signal that the aircraft is no longer
6486 under authorized control through the ANSP to the SSP. (See Secure Airspace section for concept
6487 when control cannot be restored.) Special communication channels also are installed in such
6488 aircraft, which provide secure two-way data and voice transmission from cabin and cockpit to
6489 the DSP and SSP directly in the event of a critical security incident.

6490 **8.2.2 Onboard Personnel**

6491 Although the NextGen aircraft is very well protected against the typical methods of hijack, there
6492 is still a need on certain higher risk flights for onboard LEO and other security-related personnel
6493 to guard against cabin takeovers, acts of malice (e.g., suicide bombers), or unexpected threat
6494 activities. To defend flight decks of passenger aircraft against acts of criminal violence and air
6495 piracy, personnel include specially trained flight deck crew, cabin crew staff, assigned on-board
6496 SSP personnel armed and operating clandestinely, and other armed LEOs traveling on that flight.
6497 To maintain shared situational awareness, SSP personnel have advanced communication systems
6498 that permit air-to-ground and air-to-air communication (and to the cockpit) with the ANSP, SSP
6499 and DSP. In addition, SSP personnel benefit from other NEO-based systems and programs that
6500 identify and leverage the presence of other armed LEOs as they travel on their routine business

6501 (e.g., prisoner transport) on a given flight. This information aids in scheduling mission/flight
6502 assignments for SSP LEOs. Training and USG agreements with local LEO organizations allow
6503 nonfederal LEO to assist SSP on-board LEOs. (Additional information about on-board protection
6504 is available in an **SSI** annex to this report.)

6505 **8.3 AIRCRAFT MONITORING/SURVEILLANCE**

6506 Surveillance sensors and CCTV are used to detect, monitor, and in certain cases mitigate cabin
6507 attack by passengers or by release of threat agents and aircraft use as a transport for CBRNE in
6508 at-risk aircraft. They also provide an additional data resource if hijacking/diversion of the aircraft
6509 occurs. Security sensors and surveillance are present in the flight deck, cabin, and cargo hold.
6510 The flight deck also contains the onboard control center for these systems, which is biometrically
6511 activated by authorized crew.

6512 **8.3.1 Cockpit, Cabin, and Cargo Hold Surveillance**

6513 To provide security personnel with a better understanding of the actual situation in a particular
6514 aircraft, a cockpit, cabin, and cargo hold surveillance (CCCHS) capability is incorporated in at-
6515 risk aircraft. The installed systems are completely integrated into the ANSP-provided
6516 communications and data network capabilities. They are lightweight, compact, and create no
6517 additional safety hazard to passengers, crew, or other aircraft systems. During security events,
6518 real-time video, with compression and time-limited segments, of the cockpit is compatible with
6519 flight data and voice recorder transmissions. The onboard SSP also can access security-related
6520 data streams from this system through handheld communication systems and can transmit
6521 portions of the data to the SSP SCC and SOC responsible for the flight. Thus, security personnel
6522 have a capability during security events to view in real-time the cockpit, cabin, and cargo hold
6523 surveillance videos.

6524 **8.3.2 Continuous Air Monitoring**

6525 Lightweight and safe continuous air monitoring (CAM) systems are installed in at-risk aircraft to
6526 mitigate or prevent release of CBRN threats in the cabin and cargo hold. They provide an
6527 additional security layer mitigating the use of the aircraft as a vector for transporting such threats
6528 by cargo, baggage, or by passengers themselves (e.g., bioterrorism or illness). To detect naturally
6529 occurring or criminally introduced chemical or biological (CB) threats in the cabin or cargo hold,
6530 small, lightweight advanced technology sensor systems are used in conjunction with robust
6531 NEO-based communications, installed without affecting safety. The CAM systems also have
6532 some proven crew/LEO CONOPS that may be used to flush contaminated air from the cabin or
6533 otherwise mitigate effects, and/or automated air treatment capabilities so that certain airborne
6534 threats, primarily biological, can be neutralized or sterilized to protect cabin and crew during the
6535 flight. Indicators of potentially dangerous situations (e.g., heat and smoke detectors) are
6536 leveraged off aircraft safety systems. Procedures are in place to divert aircraft suspected of
6537 contamination to appropriate facilities within the United States that are able to safely treat
6538 passengers and decontaminate aircraft.

6539 **8.4 AIRCRAFT HARDENING AND DEFENSIVE SYSTEMS**

6540 Hardening the aircraft structure, internal systems/components, and/or accessory devices (e.g.,
6541 cargo containers) can enhance aircraft security by mitigating internal explosive destruction and
6542 external attacks. Because of the expense, safety implications and difficulty of adding hardened
6543 systems to civilian aircraft, the SSP, DSP and ANSP form a collaborative research, development,
6544 test, and evaluation (RDT&E) effort to enable proof of concept, simulations and prototype
6545 development, and operational suitability assessments of various alternative designs. A particular
6546 requirement is the development of a low-cost and weight barrier to separate cargo aircraft flight
6547 decks from the cargo area.

6548 The goal is to have several preapproved (flightworthiness certified) accessory devices or design
6549 changes for at-risk aircraft types that can be retrofitted and implemented if the security situation
6550 requires it. In all cases, the priority is to leverage ongoing safety modifications for concurrent
6551 mitigation of attacks.

6552 One such example implemented in NextGen aircraft is the use of fuel and fuel tanks with
6553 enhanced resistance to explosion, while leveraging the ongoing nonexplosive fuel research. In
6554 addition to the obvious safety improvement, these approaches provide mitigation of projectile or
6555 directed energy attacks on an aircraft. New construction techniques and materials also help
6556 aircraft better tolerate internal explosions or external attacks. The overarching goal is to use the
6557 IRM model to develop high-return aircraft security enhancement and hardening elements for
6558 aircraft during airframe/system design, in lieu of retrofit design, significantly reducing cost
6559 implications.

6560 For defensive systems, leveraging safety modifications to enhance the mitigation of external
6561 threats to the aircraft is the first priority. For those aircraft types assessed at risk, NextGen
6562 aircraft design standards identify and prioritize modifications to increase shielding of critical
6563 flight systems from direct energy weapons and electromagnetic pulse (EMP) technologies and
6564 events. Procedural and operational technique training for flight crew in response to MANPADS,
6565 laser and directed energy attack are standard for NextGen aircraft assessed at risk.

6566 **8.5 SAFETY INTEGRATION**

6567 Aircraft security solutions for NextGen (e.g., systems, equipment, procedures) undergo the safety
6568 risk analysis and management process prescribed by the NextGen safety management system
6569 (SMS). The NextGen safety management process specifies a collaborative and integrated safety
6570 and security hazard/threat mitigation strategy so the security threat mitigation and safety hazard
6571 mitigation could complement, and not conflict with, each other. (See also Chapter 8, Safety
6572 Management Services of Concept of Operations Version 1.2)

6573 **References**

6574

6575 1. ASME Innovative Technologies Institute, LLC. *Risk Analysis and Management for*
6576 *Critical Asset Protection (RAMCAP) Applied to Terrorism and Homeland Security.*
6577 Version 1.1d, October 5, 2005.

6578

6579 2. *Recommended Security Guidelines for Airport Planning, Design and Construction* (TSA
6580 reference document).

6581

6582 3. RMAP and RAMCAP Risk Management references.

6583

6584 4. 49 CFR Parts 1520, 1540, 1542, et al., *Air Cargo Security Requirements*. Final Rule, May
6585 26, 2006.

6586

6587 5. *National Infrastructure Protection Plan*.