

Improving Critical Infrastructure Cybersecurity Executive Order 13636

Preliminary Cybersecurity Framework

2 **Note to Reviewers**

3 The *Preliminary Cybersecurity Framework* for improving critical infrastructure cybersecurity is
4 now available for review. The Preliminary Cybersecurity Framework is provided by the National
5 Institute of Standards and Technology (NIST).

6 If the Cybersecurity Framework is to be effective in helping to reduce cybersecurity risk to the
7 Nation’s critical infrastructure, it must be able to assist organizations in addressing a variety of
8 cybersecurity challenges. The National Institute of Standards and Technology (NIST) requests
9 that reviewers consider the following questions:

10 Does the Preliminary Framework:

- 11 • adequately define outcomes that strengthen cybersecurity and support business
12 objectives?
- 13 • enable cost-effective implementation?
- 14 • appropriately integrate cybersecurity risk into business risk?
- 15 • provide the tools for senior executives and boards of directors to understand risks and
16 mitigations at the appropriate level of detail?
- 17 • provide sufficient guidance and resources to aid businesses of all sizes while maintaining
18 flexibility?
- 19 • provide the right level of specificity and guidance for mitigating the impact of
20 cybersecurity measures on privacy and civil liberties?
- 21 • express existing practices in a manner that allows for effective use?

22
23 Will the Preliminary Framework, as presented:

- 24 • be inclusive of, and not disruptive to, effective cybersecurity practices in use today,
25 including widely-used voluntary consensus standards that are not yet final?
- 26 • enable organizations to incorporate threat information?

27
28 Is the Preliminary Framework:

- 29 • presented at the right level of specificity?
- 30 • sufficiently clear on how the privacy and civil liberties methodology is integrated with
31 the Framework Core?

32 **Disclaimer**

33 Any mention of commercial products is for information only; it does not imply NIST
34 recommendation or endorsement, nor does it imply that the products mentioned are necessarily
35 the best available for the purpose.

36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62

Table of Contents

1.0 Framework Introduction1
2.0 Framework Basics.....5
3.0 How to Use the Framework11
Appendix A: Framework Core.....13
Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program .28
Appendix C: Areas for Improvement for the Cybersecurity Framework36
Appendix D: Framework Development Methodology40
Appendix E: Glossary42
Appendix F: Acronyms44

List of Figures

Figure 1: Framework Core Structure 5
Figure 2: Profile Comparisons 8
Figure 3: Notional Information and Decision Flows within an Organization 9

List of Tables

Table 1: Framework Core 13
Table 2: Function and Category Unique Identifiers 27
Table 3: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program 28

63 **1.0 Framework Introduction**

64 The national and economic security of the United States depends on the reliable functioning of
65 critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued
66 Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity” on February 12,
67 2013.¹ This Executive Order calls for the development of a voluntary Cybersecurity Framework
68 (“Framework”) that provides a “prioritized, flexible, repeatable, performance-based, and cost-
69 effective approach” for assisting organizations responsible for critical infrastructure services to
70 manage cybersecurity risk.

71 Critical infrastructure is defined in the EO as “systems and assets, whether physical or virtual, so
72 vital to the United States that the incapacity or destruction of such systems and assets would have
73 a debilitating impact on security, national economic security, national public health or safety, or
74 any combination of those matters.” Due to the increasing pressures from external threats,
75 organizations responsible for critical infrastructure need to have a consistent and iterative
76 approach to identifying, assessing, and managing cybersecurity risk.

77 The critical infrastructure community includes public and private owners and operators, and
78 other supporting entities that play a role in securing the Nation’s infrastructure. Each sector
79 performs critical functions that are supported by information technology (IT), industrial control
80 systems (ICS) and, in many cases, both IT and ICS.² To manage cybersecurity risks, a clear
81 understanding of the security challenges and considerations specific to IT and ICS is required.
82 Because each organization’s risk is unique, along with its use of IT and ICS, the implementation
83 of the Framework will vary.

84 The Framework, developed in collaboration with industry, provides guidance to an organization
85 on managing cybersecurity risk. A key objective of the Framework is to encourage organizations
86 to consider cybersecurity risk as a priority similar to financial, safety, and operational risk while
87 factoring in larger systemic risks inherent to critical infrastructure.

88 The Framework relies on existing standards, guidance, and best practices to achieve outcomes
89 that can assist organizations in managing their cybersecurity risk. By relying on those practices
90 developed, managed, and updated by industry, the Framework will evolve with technological
91 advances and business requirements. The use of standards will enable economies of scale to
92 drive innovation and development of effective products and services that meet identified market
93 needs. Market competition also promotes faster diffusion of these technologies and realization of
94 many benefits by the stakeholders in these sectors.

95 Building off those standards, guidelines, and practices, the Framework provides a common
96 language and mechanism for organizations to: 1) describe their current cybersecurity posture; 2)
97 describe their target state for cybersecurity; 3) identify and prioritize opportunities for
98 improvement within the context of risk management; 4) assess progress toward the target state;
99 5) foster communications among internal and external stakeholders.

¹ 78 FR 11737

² The DHS CIKR program provides a listing of the sectors and their associated critical functions and value chains.
<http://www.dhs.gov/critical-infrastructure>

Preliminary Cybersecurity Framework

100 The Framework complements, and does not replace, an organization’s existing business or
101 cybersecurity risk management process and cybersecurity program. Rather, the organization can
102 use its current processes and leverage the Framework to identify opportunities to improve an
103 organization’s management of cybersecurity risk. Alternatively, an organization without an
104 existing cybersecurity program can use the Framework as a reference to establish one.

105 The goal of the open process in developing the Preliminary Framework was to develop a robust
106 technical basis to allow organizations to align this guidance with their organizational practices.
107 This Preliminary Framework is being issued for public comment for stakeholders to inform the
108 next version of the Framework that will be completed in February 2014, as required in EO
109 13636.

110 1.1 Overview of the Framework

111 The Framework is a risk-based approach composed of three parts: the Framework Core, the
112 Framework Profile, and the Framework Implementation Tiers. These components are detailed
113 below.

- 114 • The *Framework Core* is a set of cybersecurity activities and references that are common
115 across critical infrastructure sectors organized around particular outcomes. The Core
116 presents standards and best practices in a manner that allows for communication of
117 cybersecurity risk across the organization from the senior executive level to the
118 implementation/operations level. The Framework Core consists of five Functions—
119 Identify, Protect, Detect, Respond, Recover—which can provide a high-level, strategic
120 view of an organization’s management of cybersecurity risk. The Framework Core then
121 identifies underlying key Categories and Subcategories for each of these Functions, and
122 matches them with example Informative References such as existing standards,
123 guidelines, and practices for each Subcategory. This structure ties the high level strategic
124 view, outcomes and standards based actions together for a cross-organization view of
125 cybersecurity activities. For instance, for the “Protect” Function, categories include: Data
126 Security; Access Control; Awareness and Training; and Protective Technology. *ISO/IEC*
127 *27001 Control A.10.8.3* is an informative reference which supports the “Data during
128 transportation/transmission is protected to achieve confidentiality, integrity, and
129 availability goals” Subcategory of the “Data Security” Category in the “Protect”
130 Function.

131 Appendix B contains a methodology to protect privacy and civil liberties for a
132 cybersecurity program as required under the Executive Order. Organizations may already
133 have processes for addressing privacy risks such as a process for conducting privacy
134 impact assessments. The privacy methodology is designed to complement such processes
135 by highlighting privacy considerations and risks that organizations should be aware of
136 when using cybersecurity measures or controls. As organizations review and select
137 relevant categories from the Framework Core, they should review the corresponding
138 category section in the privacy methodology. These considerations provide organizations
139 with flexibility in determining how to manage privacy risk.

- 140 • A *Framework Profile* (“Profile”) represents the outcomes that a particular system or
141 organization has achieved or is expected to achieve as specified in the Framework
142 Categories and Subcategories. The Profile can be characterized as the alignment of

143 industry standards and best practices to the Framework Core in a particular
144 implementation scenario. Profiles are also used to identify opportunities for improving
145 cybersecurity by comparing a “Current” Profile with a “Target” Profile. The Profile can
146 then be used to support prioritization and measurement of progress toward the Target
147 Profile, while factoring in other business needs including cost-effectiveness and
148 innovation. In this sense, Profiles can be used to conduct self-assessments and
149 communicate within an organization or between organizations.

150 • *Framework Implementation Tiers* (“Tiers”) describe how cybersecurity risk is managed
151 by an organization. The Tier selection process considers an organization’s current risk
152 management practices, threat environment, legal and regulatory requirements,
153 business/mission objectives, and organizational constraints. Tiers describe the degree to
154 which an organization’s cybersecurity risk management practices exhibit the
155 characteristics (e.g., risk and threat aware, repeatable, and adaptive) defined in Section
156 2.3. The Tiers characterize an organization’s practices over a range, from Partial (Tier 1)
157 to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches
158 that are agile and risk-informed.

159 **1.2 Risk Management and the Cybersecurity Framework**

160 Risk management is the process of identifying, assessing, and responding to risk. Particularly
161 within critical infrastructure, organizations should understand the likelihood that a risk event will
162 occur and the resulting impact. With this information, organizations determine the acceptable
163 level of risk for IT and ICS assets and systems, expressed as their risk tolerance.

164 With an understanding of risk tolerance, organizations can prioritize systems that require
165 attention. This will enable organizations to optimize cybersecurity expenditures. Furthermore,
166 the implementation of risk management programs offers organizations the ability to quantify and
167 communicate changes to organizational cybersecurity. Risk is also a common language that can
168 be communicated to internal and external stakeholders.

169 While not a risk management process itself, the Framework uses risk management processes to
170 enable organizations to inform and prioritize decisions regarding cybersecurity. The Framework
171 utilizes risk assessment to help organizations select optimized target states for cybersecurity
172 activities. Thus, the Framework gives organizations the ability to dynamically select and direct
173 improvements in both IT and ICS cybersecurity risk management.

174 A comprehensive risk management approach provides the ability to identify, assess, respond to,
175 and monitor cybersecurity-related risks and provide organizations with the information to make
176 ongoing risk-based decisions. Examples of cybersecurity risk management processes include the
177 International Organization for Standardization (ISO) 31000, ISO 27005, NIST Special
178 Publication (SP) 800-39 and the Electricity Sector Cybersecurity Risk Management Process
179 (RMP) Guideline.

180 Within the critical infrastructure, organizations vary widely in their business models, resources,
181 risk tolerance, approaches to risk management, and effects on security, national economic
182 security, and national public health or safety. Because of these differences, the Framework is
183 risk-based to provide flexible implementation.

184 **1.3 Document Overview**

185 The remainder of this document contains the following sections and appendices:

- 186 • Section 2 describes the Framework components: the Framework Core, the Tiers, and the
187 Profiles.
- 188 • Section 3 presents examples of how the Framework can be used.
- 189 • Appendix A presents the Framework Core in a tabular format: the Functions, Categories,
190 Subcategories, and Informative References.
- 191 • Appendix B contains a methodology to protect privacy and civil liberties for a
192 cybersecurity program.
- 193 • Appendix C discusses areas for improvement in cybersecurity standards and practices
194 identified as a result of the Framework efforts to date.
- 195 • Appendix D describes the Framework development methodology.
- 196 • Appendix E contains a glossary of selected terms.
- 197 • Appendix F lists acronyms used in this document.
- 198

199 **2.0 Framework Basics**

200 The Framework provides a common language for expressing, understanding, and managing
 201 cybersecurity risk, both internally and externally. The Framework can be used to help identify
 202 and prioritize actions for reducing cybersecurity risk and is a tool for aligning policy, business,
 203 and technological approaches to managing that risk. Different types of entities — including
 204 sectors, organizations, and associations — can use the Framework for different means, including
 205 the creation of common Profiles.

206 **2.1 Framework Core**

207 The *Framework Core* provides references to cybersecurity activities and Informative References.
 208 The Framework Core is not a checklist of activities to perform; it presents key cybersecurity
 209 outcomes that are aligned with activities known to manage cybersecurity risk. These activities
 210 are mapped to a subset of commonly used standards and guidelines. The Framework Core
 211 comprises four elements—Functions, Categories, Subcategories, and Informative References—
 212 depicted in **Figure 1**:

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

213
 214 **Figure 1: Framework Core Structure**

215 The Framework Core elements work together as follows:

- 216 • **Functions** organize basic cybersecurity activities at their highest level. These Functions
 217 are: Identify, Protect, Detect, Respond, and Recover. The functions aid in communicating

Preliminary Cybersecurity Framework

218 the state of an organization’s cybersecurity activities by organizing information, enabling
219 risk management decisions, addressing threats, and improving by learning from previous
220 activities. The functions also align with existing methodologies for incident management,
221 and can be used to help show the impact of investments in cybersecurity. For example,
222 investments in planning and exercises support timely response and recovery actions,
223 resulting in reduced impact to delivery of services.

- 224 • **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes,
225 closely tied to programmatic needs and particular activities. Examples of Categories
226 include “Asset Management,” “Access Control,” and “Detection Processes.”
- 227 • **Subcategories** further subdivide a Category into high-level outcomes, but are not
228 intended to be a comprehensive set of practices to support a category. Examples of
229 subcategories include “Physical devices and systems within the organization are
230 catalogued,” “Data-at-rest is protected,” and “Notifications from the detection system are
231 investigated.”
- 232 • **Informative References** are specific sections of standards, guidelines, and practices
233 common among critical infrastructure sectors and illustrate a method to accomplish the
234 activities within each Subcategory. The Subcategories are derived from the Informative
235 References. The Informative References presented in the Framework Core are not
236 exhaustive but are example sets, and organizations are free to implement other standards,
237 guidelines, and practices.³

238 See **Appendix A** for the complete Framework Core listing. In addition, **Appendix B** provides an
239 initial methodology to help organizations identify and mitigate impacts of the Cybersecurity
240 Framework and associated information security measures or controls on privacy and civil
241 liberties.

242 The five Framework Core Functions defined below apply to both IT and ICS.

- 243 • **Identify** – Develop the institutional understanding to manage cybersecurity risk to
244 organizational systems, assets, data, and capabilities.

245 The Identify Function includes the following categories of outcomes: Asset Management,
246 Business Environment, Governance, Risk Assessment, and Risk Management
247 Strategy. The activities in the Identify Function are foundational for effective
248 implementation of the Framework. Understanding the business context, resources that
249 support critical functions and the related cybersecurity risks enable an organization to
250 focus its efforts and resources. Defining a risk management strategy enables risk
251 decisions consistent with the business needs or the organization.

- 252 • **Protect** – Develop and implement the appropriate safeguards, prioritized through the
253 organization’s risk management process, to ensure delivery of critical infrastructure
254 services.

³ NIST developed a compendium of informative references gathered from the RFI input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on stakeholder input.

Preliminary Cybersecurity Framework

255 The Protect function includes the following categories of outcomes: Access Control,
256 Awareness and Training, Data Security, Information Protection Processes and
257 Procedures, and Protective Technology. The Protect activities are performed consistent
258 with the organization’s risk strategy defined in the Identify function.

- 259 • **Detect** – Develop and implement the appropriate activities to identify the occurrence of a
260 cybersecurity event.

261 The Detect function includes the following categories of outcomes: Anomalies and
262 Events, Security Continuous Monitoring, and Detection Processes. The Detect function
263 enables timely response and the potential to limit or contain the impact of potential cyber
264 incidents.

- 265 • **Respond** – Develop and implement the appropriate activities, prioritized through the
266 organization’s risk management process (including effective planning), to take action
267 regarding a detected cybersecurity event.

268 The Respond function includes the following categories of outcomes: Response Planning,
269 Analysis, Mitigation, and Improvements. The Respond function is performed consistent
270 with the business context and risk strategy defined in the Identify function. The activities
271 in the Respond function support the ability to contain the impact of a potential
272 cybersecurity event.

- 273 • **Recover** – Develop and implement the appropriate activities, prioritized through the
274 organization’s risk management process, to restore the capabilities or critical
275 infrastructure services that were impaired through a cybersecurity event.

276 The Recover function includes the following categories of outcomes: Recovery Planning,
277 Improvements, and Communications. The activities performed in the Recover function
278 are performed consistent with the business context and risk strategy defined in the
279 Identify function. The activities in the Recover function support timely recovery to
280 normal operations to reduce the impact from a cybersecurity event.

281 **2.2 Framework Profile**

282 A Framework Profile (“Profile”) is a tool to enable organizations to establish a roadmap for
283 reducing cybersecurity risk that is well aligned with organization and sector goals, considers
284 legal/regulatory requirements and industry best practices, and reflects risk management
285 priorities. A Framework Profile can be used to describe both the current state and the desired
286 target state of specific cybersecurity activities, thus revealing gaps that should be addressed to
287 meet cybersecurity risk management objectives. **Figure 2** shows the two types of Profiles:
288 Current and Target. The Current Profile indicates the cybersecurity outcomes that are currently
289 being achieved. The Target Profile indicates the outcomes needed to achieve the desired
290 cybersecurity risk management goals. The Target Profile is built to support business/mission
291 requirements and aid in the communication of risk within and between organizations.

292 The Profile is the alignment of the Functions, Categories, Subcategories and industry standards
293 and best practices with the business requirements, risk tolerance, and resources of the
294 organization. Identifying the gaps between the Current Profile and the Target Profile allows the
295 creation of a prioritized roadmap that organizations will implement to reduce cybersecurity risk.
296 The prioritization of the gaps is driven by the organization’s Risk Management Processes and

297 serve as an essential part for resource and time estimates needed that are critical to prioritization
298 decisions.

299



Figure 2: Profile Comparisons

300

301

302

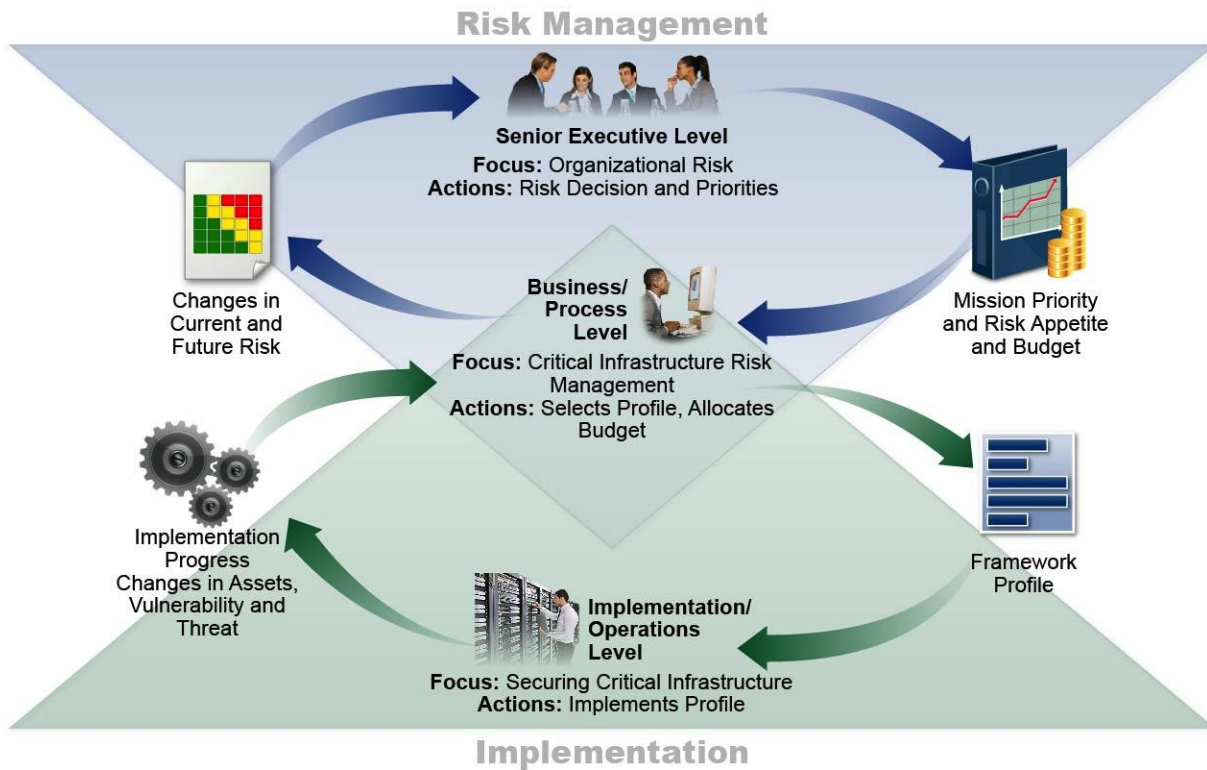
303 The Framework provides a mechanism for organizations, sectors, and other entities to create
304 their own Target Profiles. It does not provide Target Profile templates; rather, sectors and
305 organizations should identify existing Target Profiles that could be customized for their purposes
306 and needs.

307 2.3 Coordination of Framework Implementation

308 **Figure 3** describes the notional flow of information and decisions within an organization: at the
309 senior executive level, at the business/process level, and at the implementation/operations level.

310 The senior executive level communicates the mission priorities, available resources, and overall
311 risk tolerance to the business/process level. The business/process level uses the information as
312 inputs into their risk management process, and then collaborates with the
313 implementation/operations level to create a Profile. The implementation/operation level
314 communicates the Profile implementation to the business/process level. The business/process
315 level uses this information to perform an impact assessment. The outcomes of that impact
316 assessment are reported to the senior executive level to inform the organization’s overall risk
317 management process.

318



319

320

Figure 3: Notional Information and Decision Flows within an Organization

321 **2.4 Framework Implementation Tiers**

322 The Framework Implementation Tiers (“Tiers”) describe how an organization manages its
 323 cybersecurity risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an
 324 increasing degree of rigor and sophistication in cybersecurity risk management practices and the
 325 extent to which cybersecurity risk management is integrated into an organization’s overall risk
 326 management practices. The Tier selection process considers an organization’s current risk
 327 management practices, threat environment, legal and regulatory requirements, business/mission
 328 objectives, and organizational constraints. Organizations should determine the desired Tier,
 329 ensuring that the selected levels meet the organizational goals, reduce cybersecurity risk to
 330 critical infrastructure, and are feasible and cost-effective to implement. The Tier definitions are
 331 as follows:

332 • **Tier 1: Partial**

- 333 ○ Risk Management Process – Organizational cybersecurity risk management
 334 practices are not formalized and risk is managed in an ad hoc and sometimes
 335 reactive manner. Prioritization of cybersecurity activities may not be directly
 336 informed by organizational risk objectives, the threat environment, or
 337 business/mission requirements.
- 338 ○ Integrated Program – There is a limited awareness of cybersecurity risk at the
 339 organizational level and an organization-wide approach to managing
 340 cybersecurity risk has not been established. The organization implements
 341 cybersecurity risk management on an irregular, case-by-case basis due to varied

342 experience or information gained from outside sources. The organization may not
343 have processes that enable cybersecurity information to be shared within the
344 organization.

345 ○ External Participation – An organization may not have the processes in place to
346 participate in coordination or collaboration with other entities.

347 ● **Tier 2: Risk-Informed**

348 ○ Risk Management Process – Risk management practices are approved by
349 management but may not be established as organizational-wide policy.

350 ○ Integrated Program – There is an awareness of cybersecurity risk at the
351 organizational level but an organization-wide approach to managing cybersecurity
352 risk has not been established. Risk-informed, management-approved processes
353 and procedures are defined and implemented and staff has adequate resources to
354 perform their cybersecurity duties. Cybersecurity information is shared within the
355 organization on an informal basis.

356 ○ External Participation – The organization knows its role in the larger ecosystem,
357 but has not formalized its capabilities to interact and share information externally.

358 ● **Tier 3: Risk-Informed and Repeatable**

359 ○ Risk Management Process – The organization’s risk management practices are
360 formally approved and expressed as policy. Organizational cybersecurity
361 practices are regularly updated based on the application of risk management
362 processes to a changing threat and technology landscape.

363 ○ Integrated Program – There is an organization-wide approach to manage
364 cybersecurity risk. Risk-informed policies, processes, and procedures are defined,
365 implemented as intended, and validated. Consistent methods are in place to
366 effectively respond to changes in risk. Personnel possess the knowledge and skills
367 to perform their appointed roles and responsibilities.

368 ○ External Participation – The organization understands its dependencies and
369 partners and receives information from these partners enabling collaboration and
370 risk-based management decisions within the organization in response to events.

371 ● **Tier 4: Adaptive**

372 ○ Risk Management Process – The organization adapts its cybersecurity practices
373 based on lessons learned and predictive indicators derived from previous
374 cybersecurity activities. Through a process of continuous improvement, the
375 organization actively adapts to a changing cybersecurity landscape and responds
376 to emerging/evolving threats in a timely manner.

377 ○ Integrated Program – There is an organization-wide approach to managing
378 cybersecurity risk that uses risk-informed policies, processes, and procedures to
379 address potential cybersecurity events. Cybersecurity risk management is part of
380 the organizational culture and evolves from an awareness of previous activities,
381 information shared by other sources, and continuous awareness of activities on
382 their systems and networks.

- 383 ○ External Participation – The organization manages risk and actively shares
384 information with partners to ensure that accurate, current information is being
385 distributed and consumed to improve cybersecurity before an event occurs.

386 Organizations should consider leveraging external guidance, such as information that could be
387 obtained from Federal government departments and agencies, an Information Sharing and
388 Analysis Center (ISAC), existing maturity models, or other sources to assist in determining their
389 desired tier.

390 **3.0 How to Use the Framework**

391 The Framework is designed to complement existing business and cybersecurity operations. It can
392 serve as the foundation for a new cybersecurity program or a mechanism for improving an
393 existing program. The Framework provides a means of expressing cybersecurity requirements to
394 business partners and customers and can help identify gaps in an organization’s cybersecurity
395 practices. The following examples present several options for using the Framework.

396 **3.1 Basic Overview of Cybersecurity Practices**

397 Organizations can examine what capabilities they have implemented in the five high-level
398 Functions identified in the Framework Core: Identify, Protect, Detect, Respond, and Recover.
399 Organizations should have at least basic capabilities implemented in each of these areas, and can
400 begin to review what particular categories and subcategories they currently use to help achieve
401 those outcomes.

402 While it does not replace a risk management process, these Functions will provide a concise way
403 for senior executives and others to distill the fundamental concepts of cybersecurity risk so that
404 they can assess how identified risks are managed, and how their organization stacks up at a high
405 level against existing cybersecurity standards, guidelines, and practices. The Framework can also
406 help an organization answer fundamental questions, including “How are we doing?” Then, they
407 can move in a more informed way to strengthen their cybersecurity practices where and when
408 deemed necessary.

409 **3.2 Establishing or Improving a Cybersecurity Program**

410 The following recommended recursive steps illustrate how an organization could use the
411 Framework to create a new cybersecurity program or improve an existing cybersecurity program.

412 Step 1: **Identify**. The organization identifies its mission objectives, related systems and assets,
413 regulatory requirements and overall risk approach.

414 Step 2: **Create a Current Profile**. Beginning with the Categories specified in the Framework
415 Core, the organization develops a Current Profile that reflects its understanding of its current
416 cybersecurity outcomes based on its implementation of the Identify Function.

417 Step 3: **Conduct a Risk Assessment**. The organization analyzes the operational environment in
418 order to discern the likelihood of a cybersecurity event and the impact that the event could have

419 on the organization. It is important that critical infrastructure organizations seek to incorporate
420 emergent risks and outside threat data to facilitate a robust understanding of the likelihood and
421 impact of cybersecurity events.

422 **Step 4: Create a Target Profile.** The organization creates a Target Profile that focuses on the
423 assessment of the Framework Elements (e.g., Categories, Subcategories) describing the
424 organization's desired cybersecurity outcomes.

425 **Step 5: Determine, Analyze, and Prioritize Gaps.** The organization compares the Current
426 Profile and the Target Profile to determine gaps, and then determines resources necessary to
427 address the gaps. The organization creates a prioritized action plan that draws upon mission
428 drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target
429 Profile. The use of Profiles in this manner enables the organization to make informed decisions
430 about cybersecurity activities, supports cost/benefit analysis, and enables the organization to
431 perform targeted improvements.

432 **Step 6: Implement Action Plan.** The organization implements the steps defined in the action
433 plan and monitors its current cybersecurity practices against the Target Profile. For further
434 guidance, the Framework identifies Informative References regarding the practices described in
435 the Categories and Subcategories. Appendix B, the Privacy Methodology, provides guidance on
436 privacy and civil liberties considerations for the selected Categories and Subcategories.

437 **3.3 Communicating Cybersecurity Requirements with Stakeholders**

438 The Framework provides a common language to communicate requirements among
439 interdependent partners responsible for the delivery of essential critical infrastructure services.
440 Examples include:

- 441 • An organization may utilize a Target Profile to express requirements to an external
442 service provider (e.g., a cloud provider) to which it is exporting data.
- 443 • An organization may express its cybersecurity state through a Current Profile to report
444 results or for comparison with acquisition requirements.
- 445 • A critical infrastructure owner/operator, having identified an external partner on whom
446 that infrastructure depends, may use a Target Profile to convey Categories and
447 Subcategories.
- 448 • A critical infrastructure sector may establish a baseline Target Profile that can be used
449 among its constituents as an initial baseline.

450 **3.4 Identifying Opportunities for New or Revised Informative References**

451 The Framework can be used to identify opportunities for new or revised standards, guidelines, or
452 practices where additional Informative References would help organizations address emerging
453 threats. An organization implementing a given Subcategory might discover that there are few
454 Informative References, if any, for a related activity. To address that need, the organization
455 might collaborate with technology leaders and/or standards bodies to draft, develop, and
456 coordinate standards, guidelines, or practices to address the needs of potential adopters.

457 **Appendix A: Framework Core**

458 This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that
 459 describe specific cybersecurity activities that are common across all critical infrastructure sectors. The Framework Core presented in
 460 this appendix is not exhaustive; it is extensible, allowing organizations, sectors, and other entities to add Subcategories and
 461 Informative References that are relevant to them and enable them to more effectively manage their cybersecurity risk. Activities can
 462 be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative
 463 References may be added to the Profile. An organization’s risk management processes, legal/regulatory requirements,
 464 business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation.

465

466

Table 1: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (AM): The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.4 • COBIT BAI03.04, BAI09.01, BAI09, BAI09.05 • ISO/IEC 27001 A.7.1.1, A.7.1.2 • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC1
		ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.4 • COBIT BAI03.04, BAI09.01, BAI09, BAI09.05 • ISO/IEC 27001 A.7.1.1, A.7.1.2 • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC 2
		ID.AM-3: The organizational communication and data flow is mapped	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.4 • COBIT DSS05.02 • ISO/IEC 27001 A.7.1.1 • NIST SP 800-53 Rev. 4 CA-3, CM-8, CA-9 • CCS CSC 1

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
		ID.AM-4: External information systems are mapped and catalogued	<ul style="list-style-type: none"> • NIST SP 500-291 3, 4 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.6 • COBIT APO03.03, APO03.04, BAI09.02 • NIST SP 800-53 Rev. 4 RA-2, CP-2 • NIST SP 800-34 Rev 1 • ISO/IEC 27001 A.7.2.1
		ID.AM-6: Workforce roles and responsibilities for business functions, including cybersecurity, are established	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.3.3 • COBIT APO01.02, BAI01.12, DSS06.03 • ISO/IEC 27001 A.8.1.1 • NIST SP 800-53 Rev. 4 CP-2, PM-11 • NIST SP 800-34 Rev 1
	Business Environment (BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized, and inform cybersecurity roles, responsibilities, and risk decisions.	ID.BE-1: The organization’s role in the supply chain and is identified and communicated	<ul style="list-style-type: none"> • COBIT APO08.01, APO08.02, APO08.03, APO08.04, APO08.05, APO10.03, DSS01.02 • ISO/IEC 27001 A.10.2 • NIST SP 800-53 Rev. 4 CP-2
		ID.BE-2: The organization’s place in critical infrastructure and their industry ecosystem is identified and communicated	<ul style="list-style-type: none"> • COBIT APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.2.1, 4.2.3.6 • COBIT APO02.01, APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-11
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	<ul style="list-style-type: none"> • COBIT DSS01.03 • ISO/IEC 27001 9.2.2 • NIST SP 800-53 Rev 4 CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PM-8

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
Function 1	Category 1	ID.BE-5: Resilience requirements to support delivery of critical services are established	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CP-2, SA-14
		ID.GV-1: Organizational information security policy is established	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.6 • COBIT APO01.03, EA01.01 • ISO/IEC 27001 A.6.1.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
		ID.GV-2: Information security roles & responsibility are coordinated and aligned	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.3.3 • ISO/IEC 27001 A.6.1.3 • NIST SP 800-53 Rev. 4 AC-21, PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	<ul style="list-style-type: none"> • ISA 99.02.01 4.4.3.7 • COBIT MEA03.01, MEA03.04 • ISO/IEC 27001 A.15.1.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 PM-9, PM-11
Function 2	Category 2	ID.RA-1: Asset vulnerabilities are identified and documented	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • COBIT APO12.01, APO12.02, APO12.03, APO12.04 • ISO/IEC 27001 A.6.2.1, A.6.2.2, A.6.2.3 • CCS CSC4 • NIST SP 800-53 Rev. 4 CA-2, RA-3, RA-5, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources.	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001 A.13.1.2 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
		ID.RA-3: Threats to organizational assets are identified and documented	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12 • COBIT APO12.01, APO12.02, APO12.03, APO12.04 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-16
		ID.RA-4: Potential impacts are analyzed	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-3
		ID.RA-5: Risk responses are identified.	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 PM-9
	<p>Risk Management Strategy (RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	ID.RM-1: Risk management processes are managed and agreed to	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.2 • COBIT APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • NIST SP 800-53 Rev. 4 PM-9 • NIST SP 800-39
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.6.5 • COBIT APO10.04, APO10.05, APO12.06 • NIST SP 800-53 Rev. 4 PM-9 • NIST SP 800-39
		ID.RM-3: The organization’s determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11
PROTECT (PR)	<p>Access Control (AC): Access to information resources and associated facilities are limited to authorized users, processes or devices (including other information systems), and to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.3.5.1 • COBIT DSS05.04, DSS06.03 • ISO/IEC 27001 A.11 • NIST SP 800-53 Rev. 4 AC-2, AC-5, AC-6, IA Family • CCS CSC 16

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
		PR.AC-2: Physical access to resources is managed and secured	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.3.3.2, 4.3.3.3.8 • COBIT DSS01.04, DSS05.05 • ISO/IEC 27001 A.9.1, A.9.2, A.11.4, A.11.6 • NIST SP 800-53 Rev 4 PE-2, PE-3, PE-4, PE-6, PE-9
		PR.AC-3: Remote access is managed	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.3.6.6 • COBIT APO13.01, DSS01.04, DSS05.03 • ISO/IEC 27001 A.11.4, A.11.7 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.3.7.3 • ISO/IEC 27001 A.11.1.1 • NIST SP 800-53 Rev. 4 AC-3, AC-4, AC-6, AC-16 • CCS CSC 12, 15
		PR.AC-5: Network integrity is protected	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.3.4 • ISO/IEC 27001 A.10.1.4, A.11.4.5 • NIST SP 800-53 Rev 4 AC-4
	Awareness and Training (AT): The organization’s personnel and partners are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: General users are informed and trained	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.4.2 • COBIT APO07.03, BAI05.07 • ISO/IEC 27001 A.8.2.2 • NIST SP 800-53 Rev. 4 AT-2 • CCS CSC 9
		PR.AT-2: Privileged users understand roles & responsibilities	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.4.2, 4.3.2.4.3 • COBIT APO07.02 • ISO/IEC 27001 A.8.2.2 • NIST SP 800-53 Rev. 4 AT-3 • CCS CSC 9

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
		PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.4.2 • COBIT APO07.03, APO10.04, APO10.05 • ISO/IEC 27001 A.8.2.2 • NIST SP 800-53 Rev. 4 AT-3 • CCS CSC 9
		PR.AT-4: Senior executives understand roles & responsibilities	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.4.2 • COBIT APO07.03 • ISO/IEC 27001 A.8.2.2 • NIST SP 800-53 Rev. 4 AT-3 • CCS CSC 9
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.2.4.2 • COBIT APO07.03 • ISO/IEC 27001 A.8.2.2 • NIST SP 800-53 Rev. 4 AT-3 • CCS CSC 9
	Data Security (DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	<ul style="list-style-type: none"> • COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISO/IEC 27001 A.15.1.3, A.15.1.4 • CCS CSC 17 • NIST SP 800-53 Rev 4 SC-28
		PR.DS-2: Data-in-motion is secured	<ul style="list-style-type: none"> • COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISO/IEC 27001 A.10.8.3 • NIST SP 800-53 Rev. 4 SC-8 • CCS CSC 17
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	<ul style="list-style-type: none"> • COBIT BAI09.03 • ISO/IEC 27001 A.9.2.7, A.10.7.2 • NIST SP 800-53 Rev 4 PE-16, MP-6, DM-2

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
		PR.DS-4: Adequate capacity to ensure availability is maintained.	<ul style="list-style-type: none"> • COBIT APO13.01 • ISO/IEC 27001 A.10.3.1 • NIST SP 800-53 Rev 4 CP-2, SC-5
		PR.DS-5: There is protection against data leaks	<ul style="list-style-type: none"> • COBIT APO01.06 • ISO/IEC 27001 A.12.5.4 • CCS CSC 17 • NIST SP 800-53 Rev 4 AC-4, PE-19, SC-13, SI-4, SC-7, SC-8, SC-31, AC-5, AC-6, PS-6
		PR.DS-6: Intellectual property is protected	<ul style="list-style-type: none"> • COBIT APO01.03, APO10.02, APO10.04, MEA03.01
		PR.DS-7: Unnecessary assets are eliminated	<ul style="list-style-type: none"> • COBIT BAI06.01, BAI01.10 • ISO/IEC 27001 A.10.1.3 • NIST SP 800-53 Rev. 4 AC-5, AC-6
		PR.DS-8: Separate testing environments are used in system development	<ul style="list-style-type: none"> • COBIT BAI07.04 • ISO/IEC 27001 A.10.1.4 • NIST SP 800-53 Rev. 4 CM-2
		PR.DS-9: Privacy of individuals and personally identifiable information (PII) is protected	<ul style="list-style-type: none"> • COBIT BAI07.04, DSS06.03, MEA03.01 • ISO/IEC 27001 A.15.1.3 • NIST SP 800-53 Rev 4, Appendix J
	Information Protection Processes and Procedures (IP): Security policy (that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems	PR.IP-1: A baseline configuration of information technology/operational technology systems is created	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.3.2, 4.3.4.3.3 • COBIT BAI10.01, BAI10.02, BAI10.03, BAI10.05 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-7, CM-9, SA-10 • CCS CSC 3, 10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.3.3 • COBIT APO13.01

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
	and assets.		<ul style="list-style-type: none"> • ISO/IEC 27001 A.12.5.5 • NIST SP 800-53 Rev 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, PL-8 • CCS CSC 6
		PR.IP-3: Configuration change control processes are in place	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.3.2, 4.3.4.3.3 • COBIT BAI06.01, BAI01.06 • ISO/IEC 27001 A.10.1.2 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are managed	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.3.9 • COBIT APO13.01 • ISO/IEC 27001 A.10.5.1 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	<ul style="list-style-type: none"> • COBIT DSS01.04, DSS05.05 • ISO/IEC 27001 9.1.4 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Information is destroyed according to policy and requirements	<ul style="list-style-type: none"> • COBIT BAI09.03 • ISO/IEC 27001 9.2.6 • NIST SP 800-53 Rev 4 MP-6
		PR.IP-7: Protection processes are continuously improved	<ul style="list-style-type: none"> • COBIT APO11.06, DSS04.05 • NIST SP 800-53 Rev 4 PM-6, CA-2, CA-7, CP-2, IR-8, PL-2
		PR.IP-8: Information sharing occurs with appropriate parties	<ul style="list-style-type: none"> • ISO/IEC 27001 A.10 • NIST SP 800-53 Rev. 4 AC-21
		PR.IP-9: Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed	<ul style="list-style-type: none"> • COBIT DSS04.03 • ISO/IEC 27001 A.14.1 • NIST SP 800-53 Rev. 4 CP-2, IR-8

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
Protective Technology (PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.		PR.IP-10: Response plans are exercised	<ul style="list-style-type: none"> • NIST SP 800-53 Rev.4 IR-3
		PR.IP-11: Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.)	<ul style="list-style-type: none"> • COBIT APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISO/IEC 27001 8.2.3, 8.3.1 • NIST SP 800-53 Rev 4 PS Family
	Maintenance (MA): Maintenance and repairs of operational and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	<ul style="list-style-type: none"> • ISO/IEC 27001 A.9.1.1, A.9.2.4, A.10.4.1 • NIST SP 800-53 Rev 4 MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access and supports availability requirements for important operational and information systems.	<ul style="list-style-type: none"> • COBIT 5 • ISO/IEC 27001 A.9.2.4, A.11.4.4 • NIST SP 800-53 Rev 4 MA-4
		PR.PT-1: Audit and log records are stored in accordance with audit policy	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • COBIT APO11.04 • ISO/IEC 27001 A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.5, A.15.3.1 • NIST SP 800-53 Rev. 4 AU Family • CCS CSC 14
		PR.PT-2: Removable media are protected according to a specified policy	<ul style="list-style-type: none"> • COBIT DSS05.02, APO13.01 • ISO/IEC 27001 A.10.7 • NIST SP 800-53 Rev. 4 AC-19, MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is appropriately controlled	<ul style="list-style-type: none"> • CCS CSC 6 • COBIT DSS05.02 • NIST SP 800-53 Rev 4 CM-7
		PR.PT-4: Communications networks are secured	<ul style="list-style-type: none"> • COBIT DSS05.02, APO13.01 • ISO/IEC 27001 10.10.2 • NIST SP 800-53 Rev 4 AC-18

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
			<ul style="list-style-type: none"> • CCS CSC 7
		<p>PR.PT-5: Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS)</p>	<ul style="list-style-type: none"> • COBIT APO13.01, • NIST SP 800-53 Rev 4
DETECT (DE)	<p>Anomalies and Events (AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.</p>	<p>DE.AE-1: A baseline of normal operations and procedures is identified and managed</p>	<ul style="list-style-type: none"> • ISA 99.02.01 4.4.3.3 • COBIT DSS03.01 • NIST SP 800-53 Rev. 4 AC-2, SI-3, SI-4, AT-3, CM-2
		<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 SI-4, IR-4
		<p>DE.AE-3: Cybersecurity data are correlated from diverse information sources</p>	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 SI-4
		<p>DE.AE-4: Impact of potential cybersecurity events is determined.</p>	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 IR-4, SI -4
		<p>DE.AE-05: Incident alert thresholds are created</p>	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-9 • NIST SP 800-61 Rev 2
	<p>Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p>	<ul style="list-style-type: none"> • COBIT DSS05.07 • ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5 • NIST SP 800-53 Rev. 4 CM-3, CA-7, AC-2, IR-5, SC-5, SI-4 • CCS CSC 14, 16
		<p>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events</p>	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CM-3, CA-7, IR-5, PE-3, PE-6, PE-20
		<p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</p>	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 AC-2, CM-3, CA-7
		<p>DE.CM-4: Malicious code is detected</p>	<ul style="list-style-type: none"> • COBIT DSS05.01 • ISO/IEC 27001 A.10.4.1 • NIST SP 800-53 Rev 4 SI-3

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References	
			<ul style="list-style-type: none"> • CCS CSC 5 	
		DE.CM-5: Unauthorized mobile code is detected	<ul style="list-style-type: none"> • ISO/IEC 27001 A.10.4.2 • NIST SP 800-53 Rev 4 SC-18 	
		DE.CM-6: External service providers are monitored	<ul style="list-style-type: none"> • ISO/IEC 27001 A.10.2.2 • NIST SP 800-53 Rev 4 CA-7, PS-7, SI-4, SA-4, SA-9 	
		DE.CM-7: Unauthorized resources are monitored	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CM-3, CA-7, PE-3, PE-6, PE-20, SI-4 	
		DE.CM-8: Vulnerability assessments are performed	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CM-3, CA-7, CA-8, RA-5, SA-11, SA-12 	
	<p style="text-align: center;">Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.</p>		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<ul style="list-style-type: none"> • ISA 99.02.01 4.4.3.1 • COBIT DSS05.01 • NIST SP 800-53 Rev 4 IR-2, IR-4, IR-8 • CCS CSC 5
			DE.DP-2: Detection activities comply with all applicable requirements, including those related to privacy and civil liberties	<ul style="list-style-type: none"> • ISA 99.02.01 4.4.3.2 • NIST SP 800-53 Rev 4 CA-2, CA-7
			DE.DP-3: Detection processes are exercised to ensure readiness	<ul style="list-style-type: none"> • ISA 99.02.01 4.4.3.2 • NIST SP 800-53 Rev 4 PM-14
			DE.DP-4: Event detection information is communicated to appropriate parties	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CP-2, IR-8
			DE.DP-5: Detection processes are continuously improved	<ul style="list-style-type: none"> • COBIT APO11.06, DSS04.05 • NIST SP 800-53 Rev 4 PM-6, CA-2, CA-7, CP-2, IR-8, PL-2

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
RESPOND (RS)	Response Planning (RP): Response processes and procedures are maintained and tested to ensure timely response of detected cybersecurity events.	RS.PL-1: Response plan is implemented during or after an event.	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.5.1 • NIST SP 800-53 Rev. 4 CP-10, IR-4 • CCS CSC 18
	Communications (CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	<ul style="list-style-type: none"> • ISO/IEC 27001 A.13.2.1 • ISA 99.02.01 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • NIST SP 800-53 Rev 4 CP-2, IR-8
		RS.CO-2: Events are reported consistent with established criteria	<ul style="list-style-type: none"> • ISO/IEC 27001 A.13.1.1, A.13.1.2 • ISA 99.02.01 4.3.4.5.5 • NIST SP 800-53 Rev 4 IR-6, IR-8
		RS.CO-3: Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties	<ul style="list-style-type: none"> • ISO/IEC 27001 A.10
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties	<ul style="list-style-type: none"> • ISO/IEC 27001 A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8
		RS.CO-5: Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers)	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 PM-15, SI-5
	Analysis (AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from the detection system are investigated	<ul style="list-style-type: none"> • ISO/IEC 27001 A.6.2.1 • NIST SP 800-53 Rev. 4 IR-4, IR-5, PE-6, SI-4, AU-13
		RS.AN-2: Understand the impact of the incident	<ul style="list-style-type: none"> • ISO/IEC 27001 A.6.2.1 • NIST SP 800-53 Rev. 4 CP-10, IR-4
		RS.AN-3: Forensics are performed	<ul style="list-style-type: none"> • ISO/IEC 27001 A.13.2.2, A.13.2.3 • NIST SP 800-53 Rev. 4 IR-4

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
		RS.AN-4: Incidents are classified consistent with response plans	<ul style="list-style-type: none"> • ISO/IEC 27001 A.13.2.2 • ISA 99.02.01 4.3.4.5.6 • NIST SP 800-53 Rev. 4 IR-4
	Mitigation (MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	<ul style="list-style-type: none"> • ISO/IEC 27001 A.3.6, A.13.2.3 • ISA 99.02.01 4.3.4.5.6 • NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are eradicated	<ul style="list-style-type: none"> • ISA 99.02.01 4.3.4.5.6, 4.3.4.5.10 • NIST SP 800-53 Rev. 4 IR-4
	Improvements (IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	<ul style="list-style-type: none"> • ISO/IEC 27001 A.13.2.2 • ISA 99.02.01 4.3.4.5.10, 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-8
		RS.IM-2: Response strategies are updated	<ul style="list-style-type: none"> • NIST SP 800-53 Rev. 4 CP-2, IR-8
	RECOVER (RC)	Recovery Planning (RP): Recovery processes and procedures are maintained and tested to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed
Improvements (IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.		RC.IM-1: Plans are updated with lessons learned	<ul style="list-style-type: none"> • ISA 99.02.01 4.4.3.4 • COBIT BAI05.07 • ISO/IEC 27001 13.2.2 • NIST SP 800-53 Rev. 4 CP-2
		RC.IM-2: Recovery strategy is updated	<ul style="list-style-type: none"> • COBIT APO05.04, BAI07.08 • NIST SP 800-53 Rev. 4 CP-2
Communications (CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet		RC.CO-1: Public Relations are managed	<ul style="list-style-type: none"> • COBIT MEA03.02 • NIST SP 800-53 Rev. 4 IR-4, IR-8
		RC.CO-2: Reputation after an event is repaired	<ul style="list-style-type: none"> • COBIT MEA03.02

Preliminary Cybersecurity Framework

Function	Category	Subcategory	Informative References
	Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.		

467
468
469
470
471
472
473
474
475
476
477

Informative References:

- ISA 99.02.01 (2009), Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: <http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%20FISA%2099.02.01-2009>
- Control Objectives for Information and Related Technology (COBIT): <http://www.isaca.org/COBIT/Pages/default.aspx>
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103
- NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): <http://www.counciloncybersecurity.org>

Preliminary Cybersecurity Framework

478 For ease of use, each component of the Framework Core is given unique identifiers. Functions
 479 and categories each have a unique two-character identifier, as shown in the Table 1 below.
 480 Subcategories within each category are referenced numerically; the unique identifier for the
 481 Subcategory is included in Table 2.
 482
 483

Table 2: Function and Category Unique Identifiers

484

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

485 **Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity**
 486 **Program**

487 This appendix presents a methodology to address privacy and civil liberties considerations around the deployment of cybersecurity
 488 activities and in the protection of PII. This Privacy Methodology is based on the Fair Information Practice Principles (FIPPs)
 489 referenced in the Executive Order. It is organized by Function and Category to correspond with the Framework Core. Every Category
 490 may not be represented as not all Categories give rise to privacy and civil liberties risks.

491 **Table 3: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program**

Function	Category	Methodology	Informative References	
IDENTIFY	Asset Management	Identify PII of employees, customers, or other individuals that may be impacted by or connected to cybersecurity procedures, including PII that an organization processes or analyzes, or that may transit the organization’s systems, even if the organization does not retain such information.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> SE-1 Inventory of Personally Identifiable Information 	
	Business Environment	N/A	N/A	
	Governance		Identify contractual, regulatory and legal, including Constitutional, requirements that cover: i) PII identified under the Assets category; and ii) Any cybersecurity measures that may implicate protected activities, for example, interception of electronic communications under the Electronic Communications Privacy Act, or other civil liberties considerations.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> AP-1 Authority to Collect AP-2 Purpose Specification AR-1 Governance and Privacy Program AR-3 Privacy Requirements for Contractors and Service Providers
			Identify policies and procedures that address privacy or PII management practices for the PII identified under the Assets category. In connection with the organization’s cybersecurity procedures, assess whether or under which circumstances such policies and procedures: I) provide notice to and enable consent by affected individuals regarding collection, use, dissemination, and maintenance of PII, as well as mechanisms for appropriate access, correction, and redress regarding use of PII; ii) articulate the purpose or purposes for which the PII is intended to be used;	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> AP-2 Purpose Specification AR-1 Governance and Privacy Program AR-2 Privacy Impact and Risk Assessment AR-3 Privacy Requirements for Contractors and Service Providers AR-4 Privacy Monitoring and Auditing

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
		<p>iii) provide that collection of PII be directly relevant and necessary to accomplish the specified purpose(s) and that PII is only retained for as long as is necessary and permitted to fulfill the specified purpose(s);</p> <p>iv) provide that use of PII be solely for the specified purpose(s) and that sharing of PII should be for a purpose compatible with the purpose for which the PII was collected; and</p> <p>v) to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.</p>	<ul style="list-style-type: none"> • AR-5 Privacy Awareness and Training • AR-7 Privacy-Enhanced System Design and Development • AR-8 Accounting of Disclosures • IP-1 Consent • IP-2 Individual Access • IP-3 Redress • IP-4 Complaint Management • TR Transparency • TR-1 Privacy Notice • TR-3 Dissemination of Privacy Program Information • UL-1 Internal Use • UL-2 Information Sharing with Third Parties • DI-1 Data Quality • DM-1 Minimization of Personally Identifiable Information • DM-2 Data Retention and Disposal • DM-3 Minimization of PII Used in Testing, Training, and Research <p>ISO/IEC 29100</p>
	Risk Assessment	<p>Identify whether there are threats and vulnerabilities around PII as an asset. For example, PII may be targeted as the primary commodity of value or it may be targeted as a means to access other assets within the organization.</p>	<p>NIST SP 800-53 Rev. 4 Appendix J</p> <ul style="list-style-type: none"> • SE-1 Inventory of Personally Identifiable Information • AR-2 Privacy Impact and Risk Assessment <p>ISO/IEC 29100</p>
	Risk Management Strategy	<p>Determine that processes identified under the Governance category that use of PII be solely for the specified purpose(s) are part of the organization’s risk management strategy.</p>	<p>NIST SP 800-53 Rev. 4 Appendix J</p> <ul style="list-style-type: none"> • AP-2 Purpose Specification • AR-1 Governance and Privacy Program

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
			<ul style="list-style-type: none"> DM-1 Minimization of Personally Identifiable Information
PROTECT	Access Control	Limit the use and disclosure of PII to the minimum amount necessary to provide access to applications, services, and facilities.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> AR-7 Privacy-Enhanced System Design and Development DM-1 Minimization of Personally Identifiable Information
	Awareness and Training	Senior executive support is critical for building a cybersecurity culture that is respectful of privacy and civil liberties. Assign responsibility to designated personnel to implement and provide oversight for privacy policies and practices designed to minimize the impact of cybersecurity activities on privacy and civil liberties. Have regular training for employees and contractors on following such policies and practices. Make users aware of the steps they can take to protect their PII and the content of their communications, and increase transparency around privacy impacts and security practices.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> AR-1 Governance and Privacy Program AR-2 Privacy Impact and Risk Assessment AR-3 Privacy Requirements for Contractors and Service Providers AR-4 Privacy Monitoring and Auditing AR-5 Privacy Awareness and Training AR-6 Privacy Reporting ISO/IEC 29100
	Data Security	Implement appropriate safeguards at all stages of PII’s lifecycle within the organization and proportionate to the sensitivity of the PII to protect against loss, theft, unauthorized access or acquisition, disclosure, copying, use, or modification.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> AR-4 Privacy Monitoring and Auditing AR-7 Privacy-Enhanced System Design and Development AR-8 Accounting of Disclosures DM-1 Minimization of Personally Identifiable Information DM-2 Data Retention and Disposal DM-3 Minimization of PII Used in Testing, Training, and Research
	Information Protection Processes and	Securely dispose of, de-identify, or anonymize PII that is no longer needed. Regularly audit stored PII and the need for its	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> AR-1 Governance and Privacy

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
	Procedures	retention. Have policies and procedures in place to protect data and communications as appropriate according to the law during incidents and investigations handled jointly with law enforcement/government agencies.	Program <ul style="list-style-type: none"> • AR-2 Privacy Impact and Risk Assessment • DM-1 Minimization of Personally Identifiable Information • DM-2 Data Retention and Disposal ISO/IEC 29100
	Protective Technology	Audit access to databases containing PII. Consider whether PII is being logged as part of an independent audit function, and how such PII could be minimized while still implementing the cybersecurity activity effectively.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-4 Privacy Monitoring and Auditing • DM-1 Minimization of Personally Identifiable Information
DETECT	Anomalies and Events	When detecting anomalies and events, regularly review the scope of detection and filtering methods to minimize the collection or retention of PII and communications content that is not necessary to detecting the cybersecurity event. Have policies so that any PII that is collected, used, disclosed, or retained is accurate and complete.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • DI-1 Data Quality • DM-1 Minimization of Personally Identifiable Information • DM-3 Minimization of PII Used in Testing, Training, and Research • UL-1 Internal Use • UL-2 Information Sharing with Third Parties
	Security Continuous Monitoring	When performing monitoring that involves individuals or PII, regularly evaluate the effectiveness of procedures and tailor the scope to produce minimally intrusive methods of monitoring. Provide transparency into the practices.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • DM-1 Minimization of Personally Identifiable Information • DM-3 Minimization of PII Used in Testing, Training, and Research • UL-1 Internal Use • UL-2 Information Sharing with Third Parties
	Detection Processes	Establish a process to coordinate privacy personnel participation in the review of policy compliance and enforcement for detect activities.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
			<ul style="list-style-type: none">• AR-2 Privacy Impact and Risk Assessment• AR-3 Privacy Requirements for Contractors and Service Providers• AR-4 Privacy Monitoring and Auditing• AR-5 Privacy Awareness and Training• AR-7 Privacy-Enhanced System Design and Development• AR-8 Accounting of Disclosures ISO/IEC 29100

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
<p>RESPOND</p>	<p>Response Planning</p>	<p>Distinguish between an incident that puts PII at risk and one for which the organization will use PII to assist in responding to the incident. An organization may need to take different steps in its response plan depending on such differences. For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for response, an organization may need to consider how to minimize the use of PII to protect an individual’s privacy or civil liberties.</p>	<p>NIST SP 800-53 Rev. 4 Appendix J</p> <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program • AR-2 Privacy Impact and Risk Assessment • AR-4 Privacy Monitoring and Auditing • AR-5 Privacy Awareness and Training • SE-2 Privacy Incident Response • IR-1 Incident Response Policy and Procedures • IR-2 Incident Response Training • IR-3 Incident Response Testing • IR-4 Incident Handling • IR-5 Incident Monitoring • IR-6 Incident Reporting <p>ISO/IEC 29100</p>
	<p>Communications</p>	<p>Understand any mandatory obligations for reporting breaches of PII. When voluntarily sharing information about cybersecurity incidents, limit disclosure of PII or communications content to that which is necessary to describe or mitigate the incident.</p>	<p>NIST SP 800-53 Rev. 4 Appendix J</p> <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program • AR-7 Privacy-Enhanced System Design and Development • AR-8 Accounting of Disclosures • DM-1 Minimization of Personally Identifiable Information
	<p>Analysis</p>	<p>When performing forensics, only retain PII or communications content that is necessary to the investigation. Have policies so that any PII that is collected, used, disclosed, or retained is accurate and complete.</p>	<p>NIST SP 800-53 Rev. 4 Appendix J</p> <ul style="list-style-type: none"> • DM-1 Minimization of Personally Identifiable Information • DM-2 Data Retention and Disposal • DM-3 Minimization of PII Used in Testing, Training, and Research • DI-1 Data Quality

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
	Mitigation	When considering methods of incident containment, assess the impact on individuals’ privacy and civil liberties, particularly for containment methods that may involve the closure of public communication or data transmission systems. Provide transparency concerning such methods.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program • AR-2 Privacy Impact and Risk Assessment • AR-7 Privacy-Enhanced System Design and Development • SE-2 Privacy Incident Response ISO/IEC 29100
	Improvements	When considering improvements in responding to incidents involving PII, distinguish whether the incident put PII at risk, whether the organization used PII in responding to the incident, or whether the executed response plan may have otherwise impacted privacy or civil liberties.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program • AR-2 Privacy Impact and Risk Assessment • AR-4 Privacy Monitoring and Auditing • AR-5 Privacy Awareness and Training • AR-7 Privacy-Enhanced System Design and Development • AR-8 Accounting of Disclosures • SE-2 Privacy Incident Response ISO/IEC 29100
RECOVER	Recovery Planning	Distinguish between an incident that puts PII at risk and one for which the organization will use PII to assist in recovering from the incident. An organization may need to take different steps in its recovery plan depending on such differences. For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for recovery, an organization may need to consider how to minimize the use of PII to protect an individual’s privacy or civil liberties.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program • AR-2 Privacy Impact and Risk Assessment • AR-4 Privacy Monitoring and Auditing • AR-7 Privacy-Enhanced System Design and Development • AR-8 Accounting of Disclosures

Preliminary Cybersecurity Framework

Function	Category	Methodology	Informative References
			<ul style="list-style-type: none"> • SE-2 Privacy Incident Response • DM-1 Minimization of Personally Identifiable Information ISO/IEC 29100
	Improvements	When considering improvements in recovering from incidents involving PII, distinguish whether the incident put PII at risk, whether the organization used PII in recovering from the incident, or whether the executed recovery plan may have otherwise impacted privacy or civil liberties.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-1 Governance and Privacy Program • AR-2 Privacy Impact and Risk Assessment • AR-4 Privacy Monitoring and Auditing • AR-8 Accounting of Disclosures • IP-4 Complaint Management • SE-2 Privacy Incident Response ISO/IEC 29100
	Communications	Communicate the use or disclosure of PII as part of the incident and any risk mitigation strategies to maintain or rebuild trust with affected individuals, relevant stakeholders, or the wider public.	NIST SP 800-53 Rev. 4 Appendix J <ul style="list-style-type: none"> • AR-8 Accounting of Disclosures • IP-4 Complaint Management • SE-2 Privacy Incident Response • TR-1 Privacy Notice • TR-3 Dissemination of Privacy Program Information

493 **Appendix C: Areas for Improvement for the Cybersecurity**
494 **Framework**

495 Executive Order 13636 states that the Cybersecurity Framework will “identify areas for
496 improvement that should be addressed through future collaboration with particular sectors and
497 standards-developing organizations.” Based on stakeholder input, several high-priority Areas for
498 Improvement are currently identified. These initial Areas for Improvement provide a roadmap
499 for stakeholder collaboration and cooperation to further understand and/or develop new or
500 revised standards. The initial areas for improvement are as follows:

- 501 • Authentication
- 502 • Automated Indicator Sharing
- 503 • Conformity Assessment
- 504 • Cybersecurity Workforce
- 505 • Data Analytics
- 506 • International Aspects, Impacts, and Alignment
- 507 • Privacy Standards
- 508 • Supply Chains Risk Management

509 This is not intended to be an exhaustive list, but these are highlighted as important areas that
510 should be addressed in future versions of the Framework.

511 These Areas for Improvement require continued focus; they are important but evolving areas that
512 have yet to be developed or require further research and understanding. While tools,
513 methodologies, and standards exist for some of the areas, they need to become more mature,
514 available, and widely adopted. To address the Areas for Improvement the community must
515 identify primary challenges, solicit input from stakeholders to address those identified
516 challenges, and collaboratively develop and execute action plans for addressing the challenges.

517 **C.1 Authentication**

518 Authentication challenges continue to exist across the critical infrastructure. As a result,
519 inadequate authentication solutions are a commonly exploited vector of attack by adversaries.
520 Multi-Factor Authentication can assist in closing these attack vectors by requiring individuals to
521 augment passwords (“something you know”) with “something you have,” such as a token, or
522 “something you are,” such as a biometric.

523 While new solutions continue to emerge, there is only a partial framework of standards to
524 promote security and interoperability. In addition, usability has remained a significant challenge
525 for many control systems, as many of the solutions that are available today in the marketplace
526 are for standard computing platforms. Moreover, many solutions are geared only toward
527 identification of individuals; there are fewer standards-based approaches for automated device
528 authentication.

529 The inadequacy of passwords to fulfill authentication needs was a key driver behind the 2011
530 issuance of the National Strategy for Trusted Identities in Cyberspace (NSTIC), which calls upon
531 the private sector to collaborate on development of an Identity Ecosystem that raises the level of

532 trust associated with the identities of individuals, organizations, networks, services, and devices
533 online. While NSTIC is heavily focused on consumer use cases, the standards and policies that
534 emerge from the private sector-led Identity Ecosystem Steering Group (IDESG) established to
535 support the NSTIC can inform advances in authentication for critical infrastructure going
536 forward.

537 **C.2 Automated Indicator Sharing**

538 The automated sharing of indicator information is an important tool to provide organizations
539 with timely, actionable information that they can use to detect and respond to cybersecurity
540 events as they are occurring. Current sharing communities use a combination of standard and
541 proprietary mechanisms to exchange indicators. These mechanisms have differing strengths and
542 weaknesses. Standard approaches must be developed that incorporate successful practices to
543 enable sharing within and among sectors. This shared subset of indicators needs to allow for
544 extraction of indicator data as part of the analysis of cybersecurity incidents, sharing of data that
545 does not expose the organization to further risks, and automated action by receiving
546 organizations. When indicators are received by an organization, security automation technologies
547 should be able to detect past attacks, identify compromised systems, and support the detection of
548 future attacks.

549 **C.3 Conformity Assessment**

550 Industry has a long history of developing conformity assessment programs to meet society's
551 needs. For example, the independent non-profit, Snell Memorial Foundation that was established
552 in 1957 tests and certifies helmets used in motor sports for conformity to safety performance
553 standards. Snell's conformity assessments are recognized by many U.S. racing associations.
554

555 An organization can use conformity assessment activities to assess the implementation of
556 requirements related to managing cybersecurity risk. The output of conformity assessment
557 activities can enhance an organization's understanding of its implementation of a Framework
558 profile. The decisions on the type, independence, and technical rigor of conformity assessment
559 should be risk-based. The need for confidence in conformity assessment activities must be
560 balanced with cost to the private and public sectors, including direct program costs, time-to-
561 market delays, diverse global requirements, additional legal obligations, and the cost of non-
562 conformity in the market. Successful conformity assessment provides the needed level of
563 confidence, is efficient, and has a sustainable and scalable business case. Critical infrastructure's
564 evolving implementation of Framework profiles should drive the identification of private sector
565 conformity assessment activities that address the confidence and information needs of
566 stakeholders.

567 **C.4 Cybersecurity Workforce**

568 A skilled cybersecurity workforce is necessary to meet the unique cybersecurity needs of critical
569 infrastructure. While it is widely known that there is a shortage of general cybersecurity experts,
570 there is also a shortage of qualified cybersecurity experts with an understanding of the specific
571 challenges posed to critical infrastructure. As the critical infrastructure threat and technology
572 landscape evolves, the cybersecurity workforce must continue to adapt to design, develop,
573 implement, maintain and continuously improve the necessary practices within critical
574 infrastructure environments.

575
576 Efforts such as the National Centers of Academic Excellence in Information Assurance
577 Education (CAE/IAE) and the National Initiative for Cybersecurity Education (NICE) are
578 currently creating the underpinnings of a cybersecurity workforce for the future, and establishing
579 an operational, sustainable and continually improving cybersecurity education program to
580 provide a pipeline of skilled workers for the private sector and government. While progress has
581 been made through these and other programs, greater attention is needed to help organizations
582 understand their current and future cybersecurity workforce needs, and to develop hiring,
583 acquisition, and training resources to raise the level of technical competence of those who build,
584 operate, and defend systems delivering critical infrastructure services.

585 **C.5 Data Analytics**

586 Big data and the associated analytic tools coupled with the emergence of cloud, mobile, and
587 social computing offer opportunities to process and analyze structured and unstructured
588 cybersecurity-relevant data on an unprecedented scale and specificity. Issues such as situational
589 awareness of complex networks and large-scale infrastructures can be addressed. Additionally,
590 the analysis of complex behaviors in these large scale-systems can also address issues of
591 provenance, attribution, and discernment of attack patterns.

592 For the extraordinary potential of analytics to be realized, several challenges must be
593 overcome—for example, the lack of taxonomies of big data; mathematical and measurement
594 foundations; analytic tools; measurement of integrity of tools; and correlation and causation.
595 Additionally, there are privacy implications in the use of these analytic tools, such as data
596 aggregation and PII that must be addressed for legal and public confidence reasons.

597 **C.6 International Aspects, Impacts, and Alignment**

598 Globalization and advances in technology have benefited governments, economies, and society
599 as a whole, spawning unparalleled increases in innovation, competitiveness, and economic
600 growth. However, the functioning of the critical infrastructure has become dependent on these
601 enabling technologies, spurring governments around the globe to view cybersecurity increasingly
602 as a national priority. Many governments are proposing and enacting strategies, policies, laws,
603 and regulations covering a wide range of issues and placing varying degrees of requirements on
604 organizations. As many organizations, and most sectors, operate globally or rely on the
605 interconnectedness of the global digital infrastructure, many of the requirements are affecting, or
606 may affect, how organizations operate and conduct business. Diverse and unique requirements
607 can impede interoperability, produce duplication, harm cybersecurity, and hinder innovation,
608 significantly reducing the availability and use of innovative technologies to critical
609 infrastructures in all industries. This ultimately hampers the ability of critical infrastructure
610 organizations to operate globally and to effectively manage new and evolving risk. The
611 Framework is designed to allow for the use of international standards that can scale
612 internationally.

613 **C.7 Privacy Standards**

614 The FIPPs are a set of guidelines for evaluating and mitigating privacy impacts around the
615 collection, use, disclosure, and retention of PII. They are the basis for a number of laws and
616 regulations, as well as various sets of privacy principles and frameworks, including the Privacy

617 Methodology in Appendix B. Although the FIPPs provide a process for how PII should be
618 treated, they do not provide specific implementation methods or best practices. For example, in
619 Appendix B in RS.CO, it indicates that “When voluntarily sharing information about
620 cybersecurity incidents, limit disclosure of PII or communications content to that which is
621 necessary to describe or mitigate the incident.” This concept maps to certain privacy controls in
622 NIST 800-53 Rev. 4, Appendix J, however, there is no identified standard or best practice for a
623 consistent way to distinguish between necessary and unnecessary PII, such as a format standard.
624 Thus, while the Framework Core includes a broad set of informative references, the range of
625 informative references for the Privacy Methodology is limited.

626 This lack of standardization, and supporting privacy metrics, makes it difficult to assess the
627 effectiveness of organizational implementation methods. Furthermore, organizational policies are
628 often designed to address business risks that arise out of privacy violations, such as reputation or
629 liability risks, rather than focusing on minimizing the risk of harm to individuals. Although
630 research is being conducted in the public and private sectors to improve current privacy
631 practices, many gaps remain. There are few identifiable standards or best practices to mitigate
632 the impact of cybersecurity activities on individuals’ privacy and civil liberties.

633 **C.8 Supply Chain Risk Management**

634 All organizations are part of, and dependent upon, product and service supply chains. Supply
635 chains consist of organizations that design, make, source, and deliver products and services.
636 Disruptions in one part of the supply chain may have a cascading and adverse impact on
637 organizations throughout the supply chain, both up and downstream, and across multiple sectors
638 and subsectors. Although many organizations have robust internal risk management processes,
639 there remain challenges related to criticality and dependency analysis, collaboration, information
640 sharing, and trust mechanisms throughout the supply chain. As a result, organizations continue to
641 struggle to identify their risks and prioritize their actions due to these operational dependencies
642 and the weakest links are susceptible to penetration and disruption. Supply chain risk
643 management, particularly in terms of product and service integrity, is an emerging discipline
644 characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards
645 and best practices.

646 Appendix D: Framework Development Methodology

647 This Framework was developed in response to Executive Order 13636: *Improving Critical*
648 *Infrastructure Cybersecurity*⁴ and in a manner that is consistent with NIST’s mission to promote
649 U.S. innovation and industrial competitiveness.

650 Initially, NIST issued a Request for Information (RFI) in February 2013 to gather relevant input
651 from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity
652 Framework development process.⁵ The process was designed to identify existing cybersecurity
653 standards, guidelines, frameworks, and best practices that are applicable to increase the security
654 of critical infrastructure sectors and other interested entities. NIST shared publicly the 245
655 responses to the RFI.⁶ NIST conducted an analysis of these comments, and shared initial findings
656 on May 15, 2013.⁷

657 On April 3, 2013 NIST hosted an initial workshop in Washington D.C. to identify existing
658 resources and gaps, and prioritize issues to be addressed as part of the Framework.⁸

659 At a second workshop hosted by Carnegie Mellon University, NIST worked with stakeholders to
660 discuss the foundations of the Framework and the initial analysis.⁹ The feedback from the second
661 workshop led to the development of a draft outline of the Preliminary Framework presented on
662 July 1, 2013.¹⁰

663 At a third workshop hosted by the University of California, San Diego,¹¹ the draft outline was
664 presented for validation and stakeholders contributed input to the Framework Core, which was
665 also shared publicly on July 1st.¹²

666 At the fourth workshop hosted by the University of Texas at Dallas, the discussion draft of the
667 Preliminary Framework was presented for stakeholder input.

668 Through the processes, with NIST as a convener and coordinator, the following goals were
669 developed for the Framework:

- 670 • Be an adaptable, flexible, and scalable tool for voluntary use;
- 671 • Assist in assessing, measuring, evaluating, and improving an organization’s readiness to
672 deal with cybersecurity risk;
- 673 • Be actionable across an organization;
- 674 • Be prioritized, flexible, repeatable, performance-based, and cost-effective;
- 675 • Rely on standards, methodologies, and processes that align with policy, business, and
676 technological approaches to cybersecurity;

4 <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

5 <https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity>

6 http://csrc.nist.gov/cyberframework/rfi_comments.html

7 <http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf>

8 <http://www.nist.gov/itl/csd/cybersecurity-framework-workshop.cfm>

9 <http://www.nist.gov/itl/csd/cybersecurity-framework-workshop-may-29-31-2013.cfm>

10 http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf

11 <http://www.nist.gov/itl/csd/3rd-cybersecurity-framework-workshop-july-10-12-2013-san-diego-ca.cfm>

12 http://www.nist.gov/itl/upload/draft_framework_core.pdf

Preliminary Cybersecurity Framework

- 677 • Complement rather than conflict with current regulatory authorities;
- 678 • Promote, rather than constrain, technological innovation in this dynamic arena;
- 679 • Focus on outcomes;
- 680 • Raise awareness and appreciation for the challenges of cybersecurity but also the means
- 681 for understanding and managing the related risks;
- 682 • Be consistent with voluntary international standards.
- 683
- 684
- 685

686 **Appendix E: Glossary**

687 This appendix defines selected terms used in the publication.

688 **Category:** The subdivision of a Function into groups of cybersecurity activities, closely tied to
689 programmatic needs. Examples of Categories include “Asset Management,” “Access Control,”
690 and “Detection Processes.”

691 **Critical Infrastructure:** Systems and assets, whether physical or virtual, so vital to the United
692 States that the incapacity or destruction of such systems and assets would have a debilitating
693 impact on cybersecurity, national economic security, national public health or safety, or any
694 combination of those matters.

695 **Cybersecurity Event:** A cybersecurity change that may have an impact on organizational
696 operations (including mission, capabilities, or reputation).

697 **Detect (function):** Develop and implement the appropriate activities to identify the occurrence
698 of a cybersecurity event.

699 **Framework:** A risk-based approach to reduce cybersecurity risk composed of three parts: the
700 Framework Core, the Framework Implementation Tiers, and the Framework Profile. Also known
701 as the “Cybersecurity Framework.”

702 **Framework Core:** An outcome-based compilation of cybersecurity activities and references that
703 are common across critical infrastructure sectors. The Framework Core comprises four types of
704 elements: Functions, Categories, Subcategories, and Informative References.

705 **Framework Implementation Tier:** The degree to which an organization’s cybersecurity risk
706 management practices exhibit selected desirable characteristics, such as being risk and threat
707 aware, repeatable, and adaptive.

708 **Framework Profile:** A representation of the outcomes that a particular system or organization
709 has achieved or is expected to achieve as specified in the Framework Categories and
710 Subcategories.

711 **Function:** One of the main components of the Framework. Functions provide the highest level
712 of structure for organizing cybersecurity activities into Categories and Subcategories. The five
713 functions are: Identify, Protect, Detect, Respond, and Recover.

714 **Identify (function):** Develop the institutional understanding to manage cybersecurity risk to
715 organizational systems, assets, data, and capabilities.

716 **Informative Reference:** A specific section of existing standards and practices that are common
717 among all critical infrastructure sectors and illustrate a method to accomplish the activities
718 within each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control
719 A.10 - Cryptographic technology, which supports the “Protect Data in Transit” Subcategory of
720 the “Data Security” Category in the “Protect” function.

721 **Personally Identifiable Information (or PII):** Information which can be used to distinguish or
722 trace an individual’s identity such as the individual’s name, social security number, biometric
723 records, etc., alone, or when combined with other personal or identifying information which is
724 linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name,
725 etc.

Preliminary Cybersecurity Framework

- 726
- 727 **Protect (function):** Develop and implement the appropriate safeguards, prioritized through the
728 organization’s risk management process, to ensure delivery of critical infrastructure services.
- 729 **Recover (function):** Develop and implement the appropriate activities, prioritized through the
730 organization’s risk management process, to restore the appropriate capabilities that were
731 impaired through a cybersecurity event.
- 732 **Respond (function):** Develop and implement the appropriate activities, prioritized through the
733 organization’s risk management process (including effective planning), to take action regarding a
734 detected cybersecurity event.
- 735 **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or
736 event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or
737 event occurs; and (ii) the likelihood of occurrence.
- 738 **Risk Management:** The process of identifying, assessing, and responding to risk.
- 739 **Subcategory:** The subdivision of a Category into high-level outcomes. Examples of
740 subcategories include “Physical devices and systems within the organization are catalogued,”
741 “Data-at-rest is protected,” and “Notifications from the detection system are investigated.”
- 742

743 **Appendix F: Acronyms**

744

745 This appendix defines selected acronyms used in the publication.

746

747 **CCS** Council on CyberSecurity

748 **COBIT** Control Objectives for Information and Related Technology

749 **DHS** Department of Homeland Security

750 **EO** Executive Order

751 **FIPPs** Fair Information Practice Principles

752 **ICS** Industrial Control Systems

753 **IDESG** Identity Ecosystem Steering Group

754 **IEC** International Electrotechnical Commission

755 **IR** Interagency Report

756 **ISA** International Society of Automation

757 **ISAC** Information Sharing and Analysis Center

758 **ISO** International Organization for Standardization

759 **IT** Information Technology

760 **NIST** National Institute of Standards and Technology

761 **NSTIC** National Strategy for Trusted Identities in Cyberspace

762 **OT** Operational Technology

763 **PII** Personally Identifiable Information

764 **RFI** Request for Information

765 **RMP** Risk Management Process

766 **SCADA** Supervisory Control and Data Acquisition

767 **SP** Special Publication