RG-5.71
Cyber Security Programs for Nuclear Facilities
(DG-5022)

Karl Sturzebecher
Digital Instrumentation and Controls Branch
Division of Engineering
Office of Nuclear Regulatory Research

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- RG-5.71 Development
- Technical Approach
- Path Forward
- Backup Slides
  - Comment Response
  - NUREG/CR 6847

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RG-5.71 Development

New Rule 10 CFR 73.54

- Protection of digital computer and communication systems and networks from cyber attacks
  - Safety-related and important to safety functions
  - Security functions
  - Emergency preparedness functions
  - Support systems, which if compromised, impact above

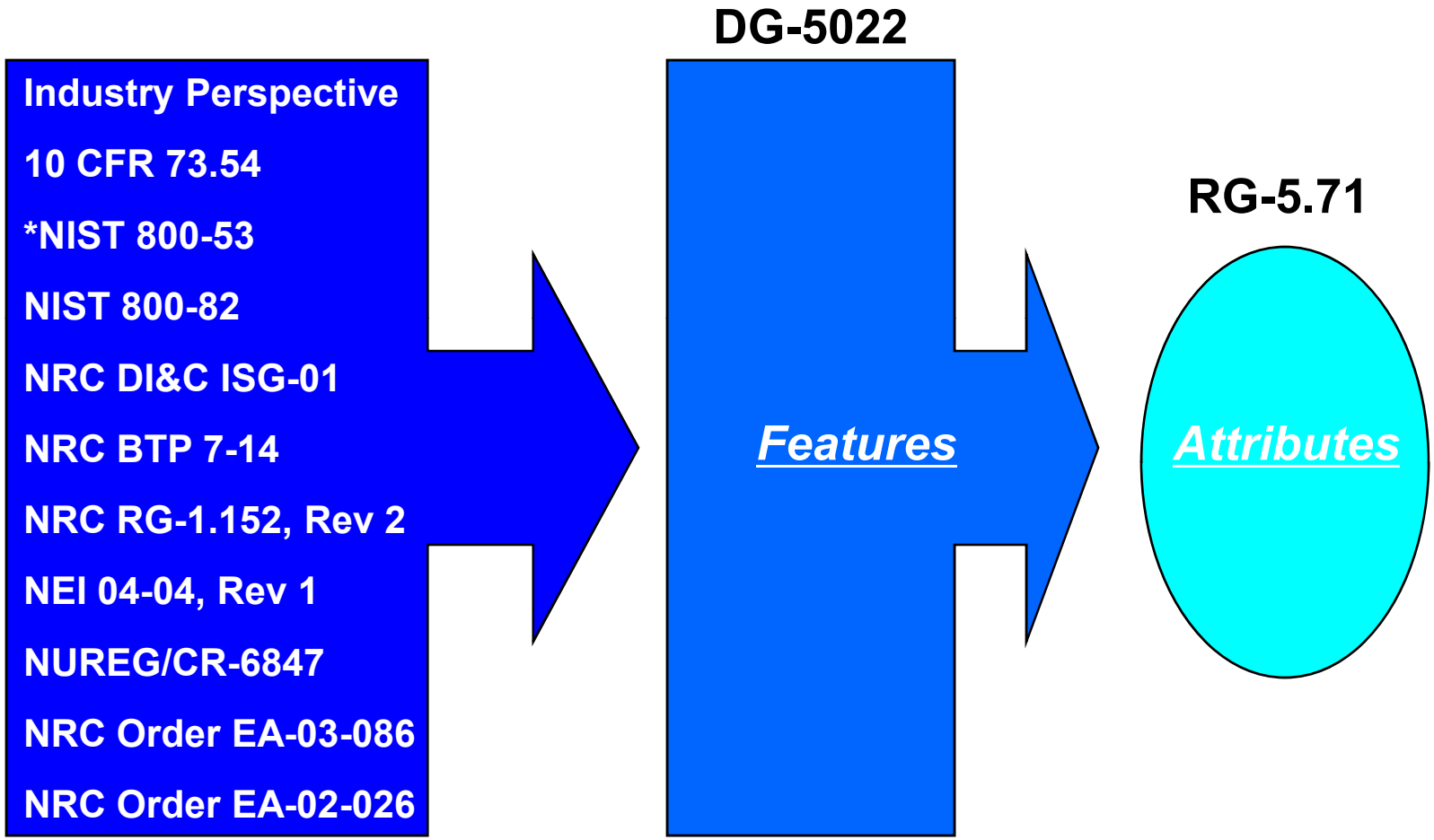
- Approved by Commission 1/09

- Anticipate OMB approval April/May

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RG-5.71 Development

Conceptual Development



*Merger of IEC 15408 (Parts 1-3) and IEC 17799

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RG-5.71 Development

Stakeholder Comments

- Participation by NERC, FERC, DHS, NIST, Joe Weiss, vendors, licensees, NEI
- 7/11/08 Stakeholder Meeting (208 comments)
  - High number of questions, assumptions, move and delete comments
- 12/4/08 Stakeholder Meeting (14 comments)
  - Cyber security plan needs to be clearer
  - Should leverage existing NRC/industry regulations, programs, and processes
  - Should use a graded approach
  - Physical and logical security boundaries do not have a one-to-one correspondence
- 1/12/09 Stakeholder Meeting (6 comments)
  - Reorganize document to discuss plan first, next program, then security controls
  - Emphasize performance-based attributes
- 2/11/09 Stakeholder Meeting (final closure)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach

Time Frame	Security Engineering Paradigm	Technical Environment
1960s – 1970s	COMPUSEC – computer security COMSEC – communications security	Digital mainframes Analog communications
1980s – mid 1990s	INFOSEC – information security	Distributed computing LANs Digital communications
Mid 1990s – today	Cyber security -Management controls -Operational controls -Technical controls	Convergence of computing and telecommunications Advances in digital technology, ASICS, PLDs, FPGAs, etc.

Cyber security: combination of : (1) inherent technical features and functions that collectively contribute to a system, system of systems, and enterprise achieving and sustaining confidentiality, integrity, and availability, and (2) implementation of standardized operational and management controls that define the nature and frequency of interaction between users, systems, and system resources, the purpose of which is to achieve and sustain and known secure state at all times, and prevent accidental and intentional theft, destruction, alteration or sabotage of system resources.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach

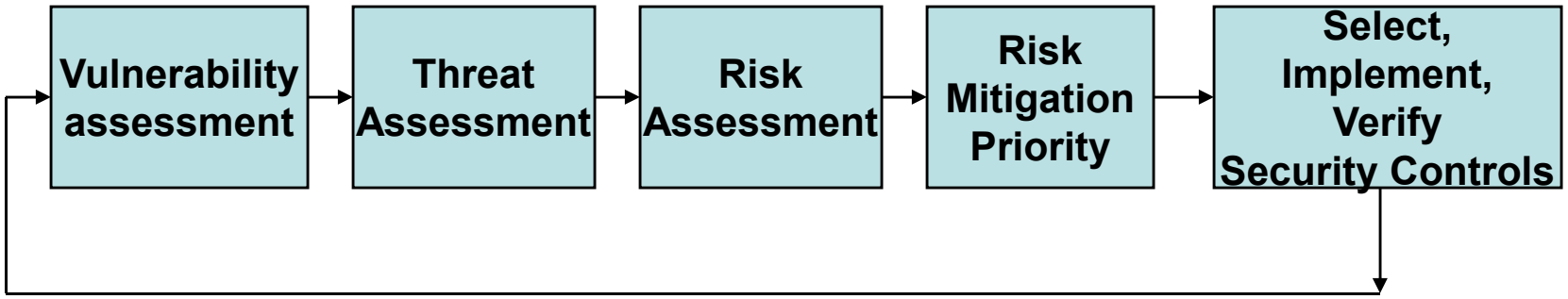
Purpose of RG-5.71

- Per 10 CFR 73.54 establish performance based requirements to ensure that the functions of critical systems and critical digital assets are protected from cyber attack throughout the system engineering lifecycle, using a graded approach

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

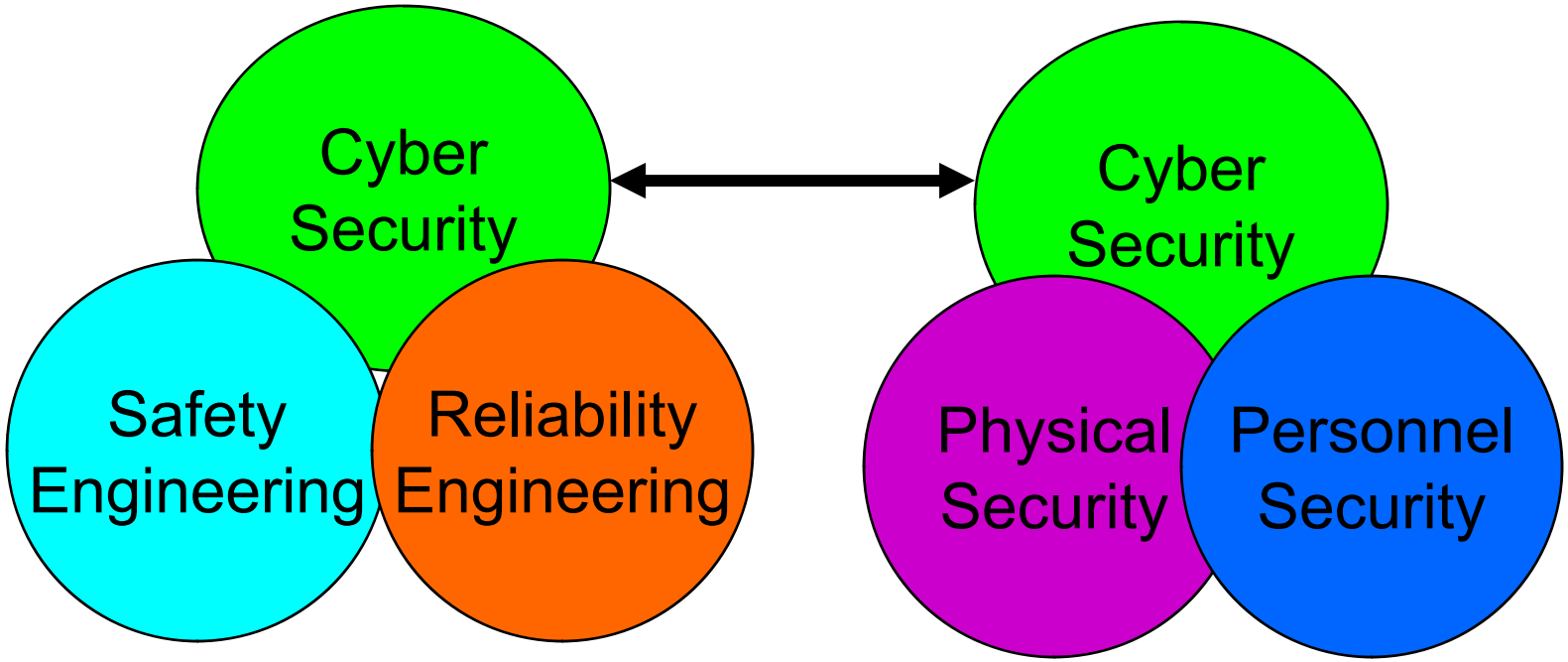
Technical Approach (3.1, 3.9)

- **Vulnerability**
  - Inherent weakness in a system, system of systems, or enterprise, its design, implementation, operation, or operational environment
- **Threat**
  - Potential for a vulnerability to be exploited, accidentally or intentionally, a function of the opportunity, motive, expertise, and resources (OMER) needed and available to effect the exploitation
- **Risk**
  - Likelihood of a vulnerability being exploited and a threat instantiated, plus the worst-case severity consequences



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

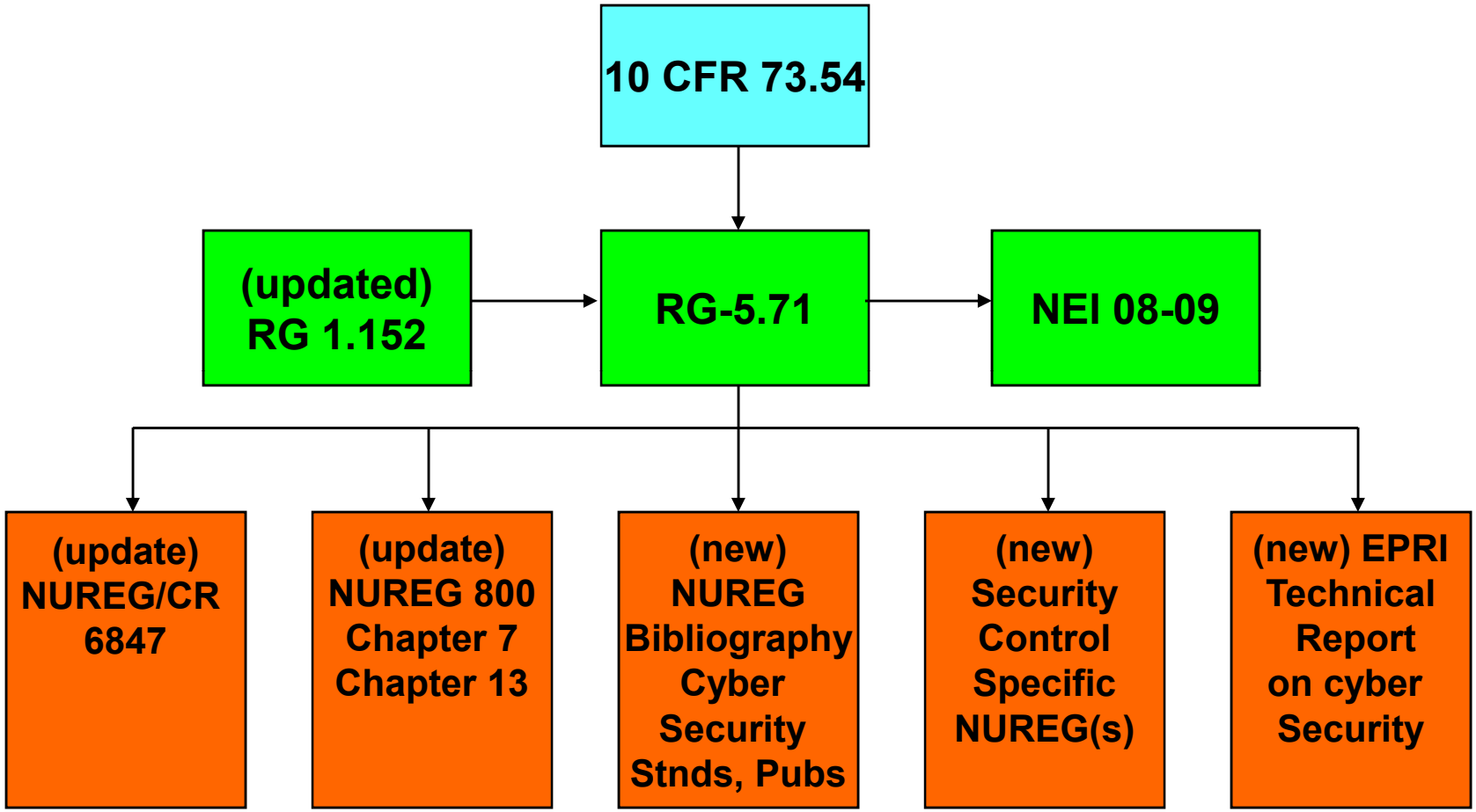
Technical Approach (3.4.1.2)



3.4.1.2 The licensee should perform concurrent security engineering lifecycle activities, to achieve high assurance that safety, reliability, and security engineering activities are coordinated.

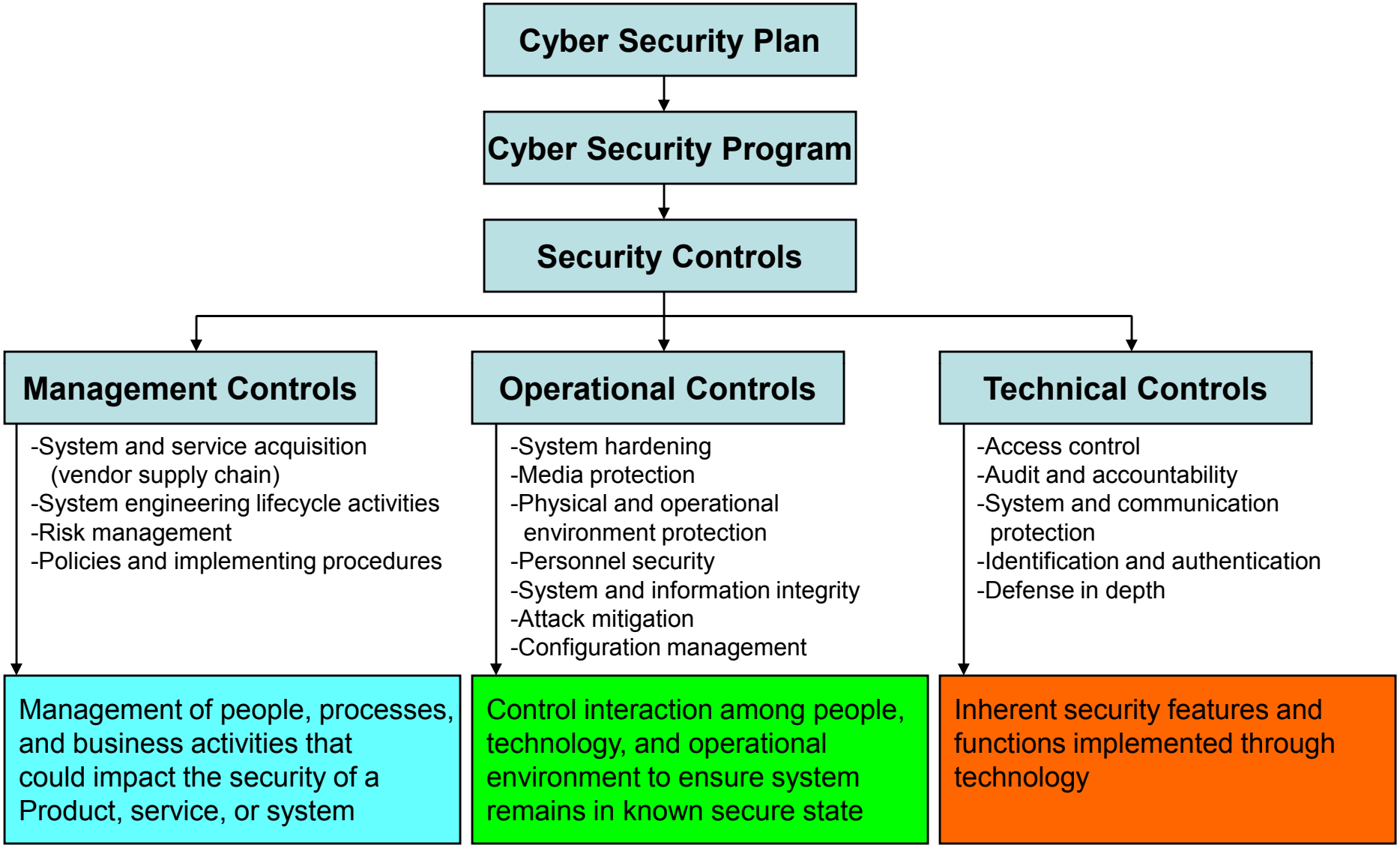
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach (3.4)



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach

Performance based

- RG-5.71 specifies attributes ("what") for which applicant must demonstrate high assurance
- Cyber security plan, policies, and implementing procedures specify details ("how"), along with applicable NUREGs
- Rationale:
  - Security architecture is site specific, tied to each system, its design, implementation, operation, and operational environment
  - Security engineering is a concurrent engineering activity, ties into existing system engineering methodology and business practices
  - Rapid evolution of cyber security technology
  - Constantly changing attack methods and threat environment
  - Security sensitive information doesn't belong in a public document
  - Approach is similar to other federal security rules and NERC cyber security standards

- " …defense technologies are widely available to mitigate threats but have not been uniformly adopted due to associated costs, perceived need, operational requirements, and regulatory constraints."
  - Director of National Intelligence Annual Threat Assessment, provided to U.S. Senate Select Committee on Intelligence, 2/12/09, p. 39.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach (3.6)

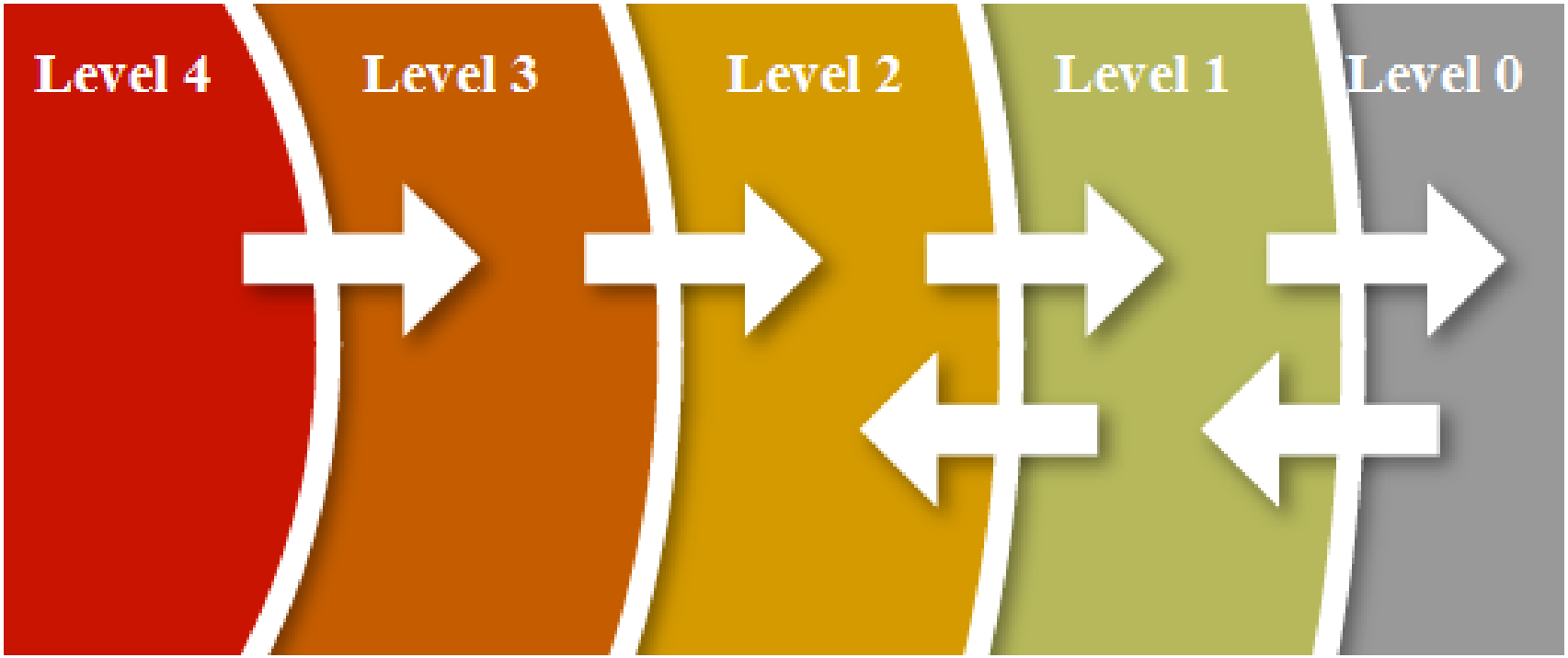
Most Common Categories of Exploits (accidental or intentional)

-Action, command, response triggering	-Masquerading, IP spoofing
-Blocking access to system resources	-Modification of information or commands
-Browsing, surveillance (pre-cursor event)	-Lack of fault tolerance, error detection or correction
-Corruption of resource management information	-Overwriting information or commands
-Deletion of information	-Password guessing, spoofing, compromise
-Denial of service, network flooding, system saturation, lack of capacity planning	-Replay, reroute, misroute messages
-EMI/RFI	-Site or system specific vulnerabilities
-Environmental, facility, power faults or tampering	-Theft of information or service
-Illegal operations, transactions, modes/states	-Trojan horse
-Inference, aggregation	-Unauthorized access or use of system resources
-Insertion of bogus data or commands	-Uncontrolled, unprotected portable systems, media, archives, hardcopies
-Lack of contingency planning, back-ups	-Unpredictable COTS behavior
	-Virus, worm, zombie, bot net

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach (3.5)

An example of such a defensive architecture is one that includes a series of concentric defensive levels of increasing security



Security Architecture: Concentric Ring Model

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach (3.5)

ISO/OSI Reference Model	Sample Protocols	Sample Security Controls
7: Application Layer	FTP, HTTP, SMTP, SNMP, Telnet, APIs	Prohibit use of Telnet, require HTTPS, Digital certificates, system hardening
6: Presentation	Context and syntax management	**Information hiding**
5: Session	Session management and Synchronization	Digital certificates
4: Transport	TCP, UDP	**Peer entity authentication**
3: Network	IP, X.25, ATM	IPSec, **partitioning, wrappers**
2: Data Link	IEEE 802.3, Frame relay	Asymmetric block encryption
1: Physical	V.90, OC-3, SONET, RS-422	Electrically isolate signals, channels, etc.

Defense in depth strategy: apply multiple different technical and operational security controls to all layers of the protocol stack.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach

Sample Implementation of Technical Controls

Access Control 3.4.3.1	Authentication 3.4.3.4
• Domain and type enforcement • Least privilege • Wrappers • Role based • Time based • Origin based • Encryption • Information hiding • Partitioning	• Biometrics • Data origin • Digital certificate • Kerberos • Unilateral • Mutual • Peer entity • Smart cards • Non-repudiation of origin, receipt

Arbitrate initiator request (person or process) to perform an operation on a target resource

Establish the claimed identity of a user, process, device, or other entity

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Approach (3.3)

Incorporating the Cyber Security Program into the Physical Protection Program

10 CFR 73.54(b)(3) security program a component of the physical protection program

- Security organization is responsible for protecting the facility from physical and cyber attacks up to and including the design-basis threat
- Align key personnel who are responsible for the management and oversight of the licensee's cyber security program
- Flexibility in regard to solid line/dotted line reporting chain

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Path Forward

RG-5.71 Next Steps

- Respond to ACRS comments
- Complete development of generic cyber security plan template NEI-08-09
- Conduct licensing reviews
- Develop and implement oversight process

Requesting ACRS letter endorsing issuance for use

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Backup: Comment Response

- **Cyber security should not be located in the physical security organization.**
  - Response: The rule, specifically 10 CFR 73.54(b)(3) requires this. However, we understand this concern and have allowed flexibility in regard to the dotted line/solid line reporting structure between cyber and physical security.

- **Need to ensure that cyber security requirements are carried forward all through the supply chain.**
  - Response: We will add "..including all suppliers, vendors, and maintenance contractors." to the end of the first bullet under 3.4.1.1. We will reword the second bullet under 3.4.1.1 to read "…vendor, supplier, and maintenance security and development lifecycles."

- **Need to emphasize the importance of configuration management, especially during hardware/software upgrades.**
  - Response: We believe the configuration management requirements stated in 3.4.1.2, which references Chapter 7 of the SRP and BTP-14, 10 CFR 54, 10 CFR 59, and section 3.10 of this document, address this concern.

- **Need to add more definitions in the glossary.**
  - Response: The additional definitions provided in this slide set will be added to the glossary.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Backup: Comment Response

- **Need to include more examples and diagrams**
  - Response: The new diagrams and tables provided on slides 8-11 and 13-16 will be added to the document.

- **Need to emphasize the deliberate exploitation of vulnerabilities.**
  - Response: This point has been added to slides 8 and 13, which will be added to the document.

- **Need to add acceptance criteria**
  - Response: The burden of proof that a security control or set of controls is acceptable and meets the high assurance test lies with the applicant. That said, a security control would be considered acceptable if:
    - The security control selected is appropriate for the vulnerability it is intended to mitigate.
    - The implementation, configuration, operation, and execution of the security control are sufficiently robust and resilient to mitigate the threat of the vulnerability being exploited.
    - The implementation, configuration, operation, and execution of the security control are consistent with industry best practices, national and international consensus standards, applicable NUREGs, site specific policies and procedures, and the due diligence criteria.
    - The security control is consistent and compatible with the overall site security architecture
  - [This statement will be added as the third paragraph in Section 3.4.]

Due diligence: (Black's Law Dictionary) such a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent person under the particular circumstances, not measured by any absolute standard, but depending on the relative facts of the special case.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Backup: NUREG/CR 6847