Donald Harriss

NIST PSCR

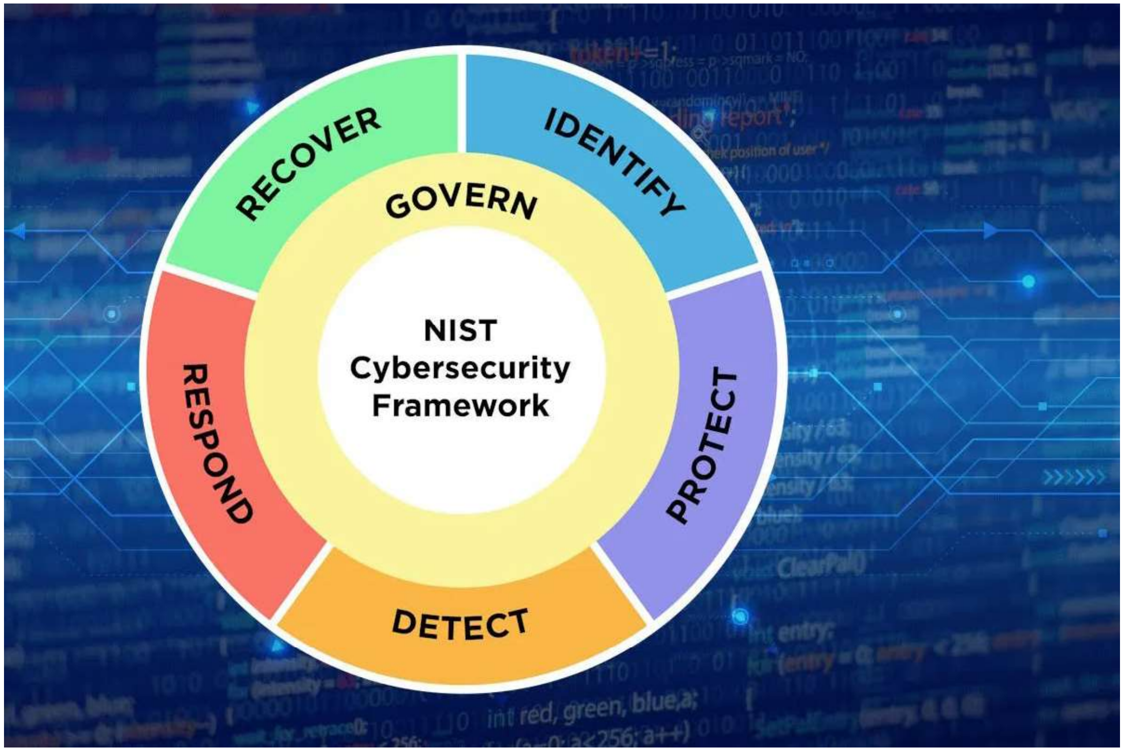
NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

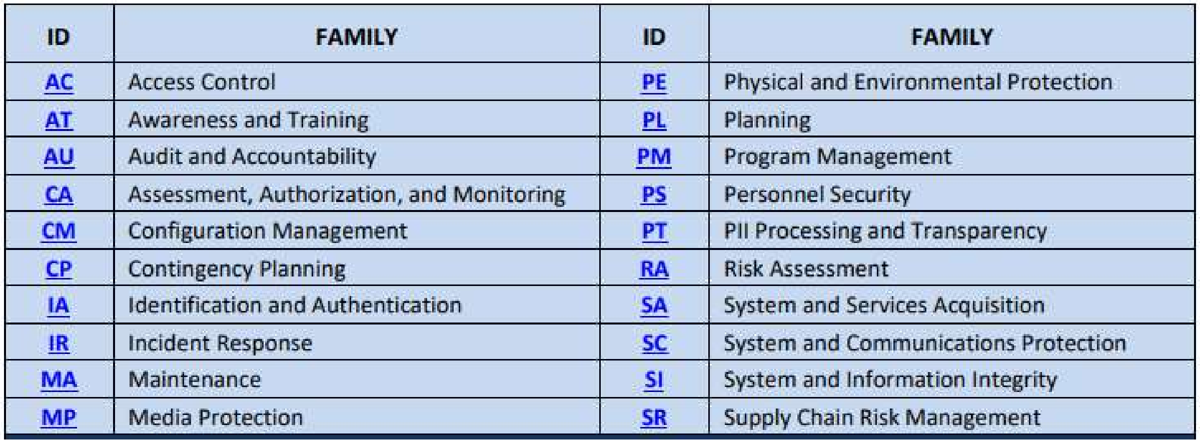
Security and Privacy Controls for Information Systems

Don Harriss

NIST PSCR UAS Technical Lead



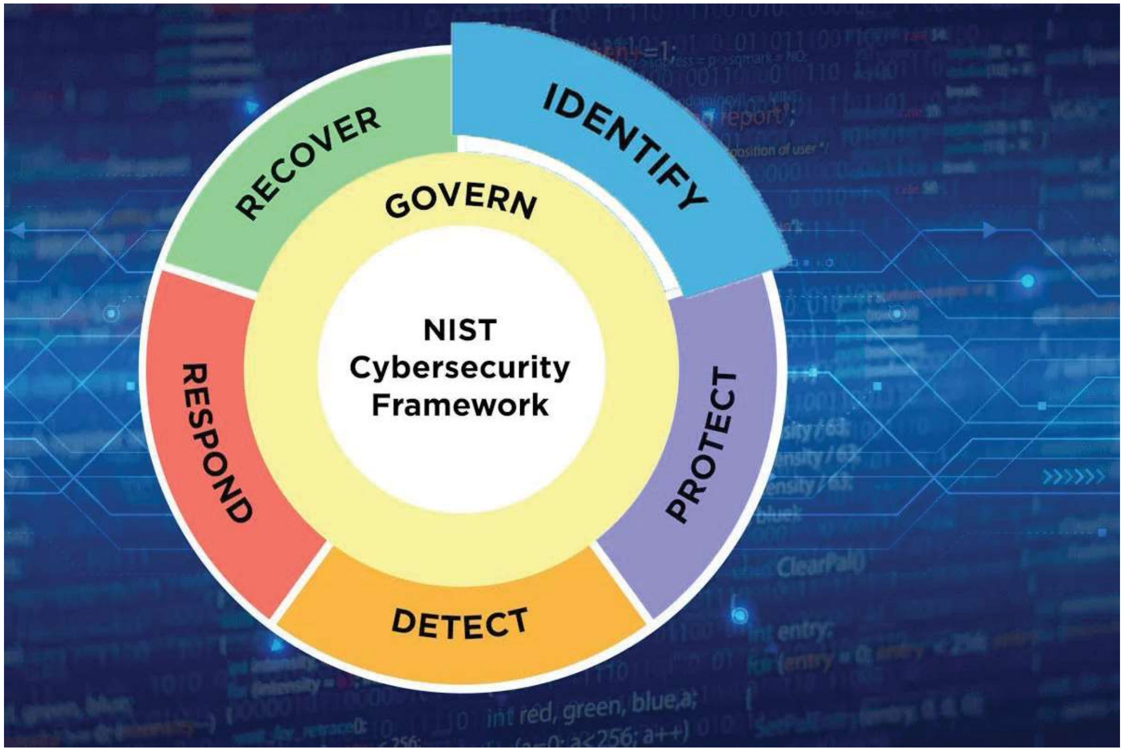
- CFS Functions Correlation to Security and Privacy Controls for Information Systems and Organizations NIST SP 800-53
- Supports the identification of security and privacy controls needed to manage risk
- Meets current and future protection needs
- Identify - Protect - Recover



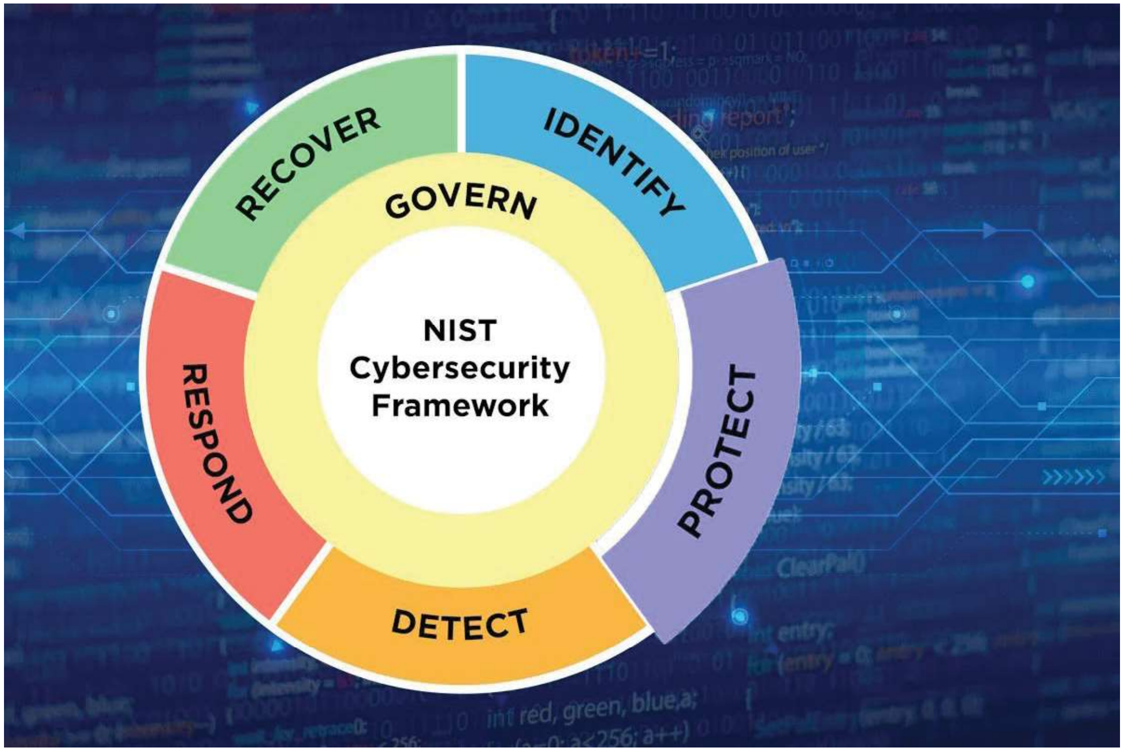
ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Security and Privacy Control Families,
NIST SP 800-53

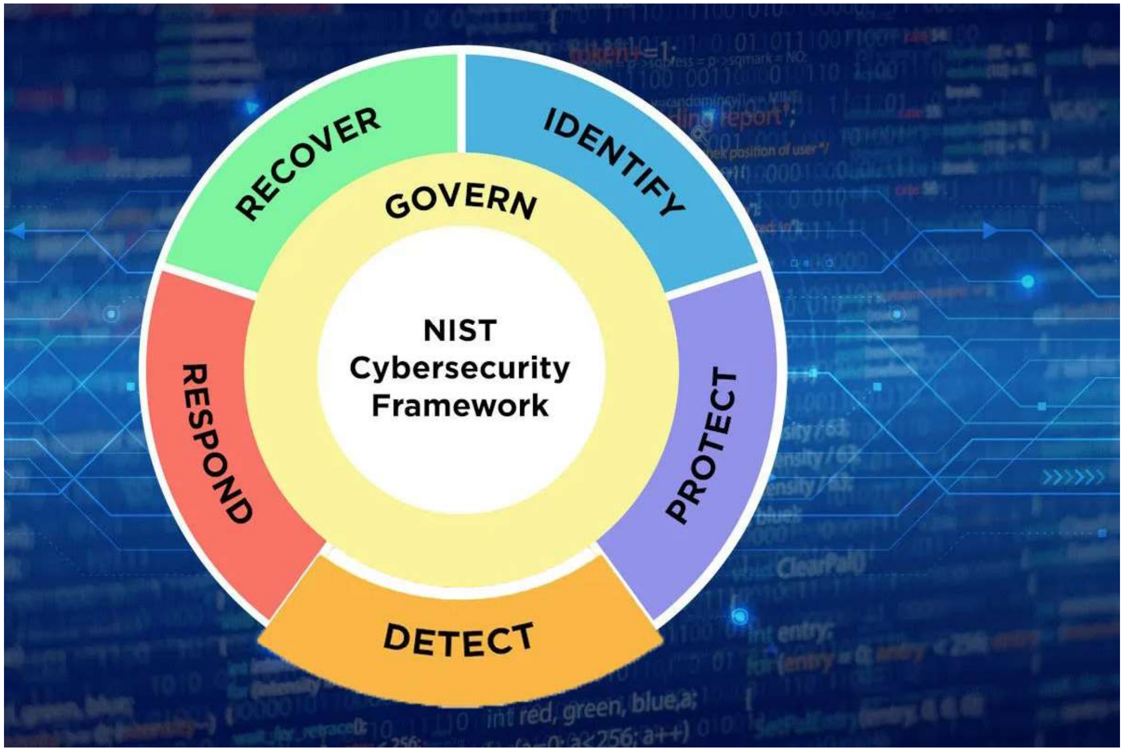
- Each family contains base controls and enhancements to provide greater protection integrity
- A control contains definitions and high-level technical discussions of the control
- Defines implementation role responsibilities and approaches
- Controls are agnostic to specific systems



- Auditing known assets
- Risk Assessment
- Supply Chain Risk Management
- Sensitive Information
- Physical and Cyber Assets
- Improvements
- Contingency Planning



- Access Controls
- Identification and Authentication
- Platform Security
- Data Protection
- Maintenance
- Technology Resilience
- Awareness and Training
- Configuration Management
- System Integrity



- Audit and Accountability
- Authorization and Monitoring
- Event Analysis

Secure Configuration

UAS and AI Implications

- Vetting of applications and software sources
- Hardware and software trusted supply chain
- Secure on-premise and cloud assets
- Secure credentialing databases
- Data protection
- Physical asset security

AI Cybersecurity Applications

Identification of People - Identity Management

Identification of Devices

Credentialing Mechanisms

Federation

- AI is an application that requires securing as well as a tool to provide security
- AI can supplement and provide enhancement for security analyst
- Detect threats
- AI applications still require security and privacy controls

AI Security Controls

Thank You

NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH