CYBERSECURITY IS A PROGRAM:

Coordinating Contractual & Regulatory Compliance for DoD Contractors

Wyoming Cybersecurity Symposium, October 23, 2019

PANELISTS:

BILL TAYLOR

Managing Director, Flatwater Forensics LLC

btaylor@flatwaterforensics.com

DAVID ASCHKINASI

Special Counsel, Glade Voogt Lopez & Smith PC

daschkinasi@gvlslaw.com

ED FULLER

Director of InfoSec, Flatwater Forensics LLC

efuller@flatwaterforensics.com

CONTRACTUAL CONTROLS.

Understanding Common Cyber Clauses:

NIST CSF	NIST Cybersecurity Framework
NIST SP 800-53r5	Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-66r1	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
NIST SP 800-171r1	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST SP 800-171A	Assessing Security Requirements for Controlled Unclassified Information
48 CFR 252.239-7010	Cloud Computing Services - Level 4 - Required Controls
ISO/IEC 27001 Controls	Information Technology - Security Techniques - Information Security Management Systems - Requirements

IT’S IN YOUR BID.

DoD InfoSec Requirements will be Identified and Audited

Common Bid Solicitation DFARS Clause:

> **DFARS 252.204-7008(c)(1):** By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

ADEQUATE CYBERSECURITY DEFINED.

DFARS 252.204-7012

(b) ***Adequate security.*** The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

YOUR SUBS OFTEN MUST COMPLY.

Both DFARS and NIST Contain Significant “Flow Down” Requirements, Critical to Contractors with Supply Chains

DFARS 252.204-7012(m):

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer;

NIST Special Publication 800-171:

Contractors and Sub-Contractors working with the Department of Defense must comply with the NIST standard for appropriately handling Controlled Unclassified Information (CUI). There are additional standards for dealing with Controlled Technical Information (CTI) which generally may be thought of as classified information. These standards are described in SP 800-171.

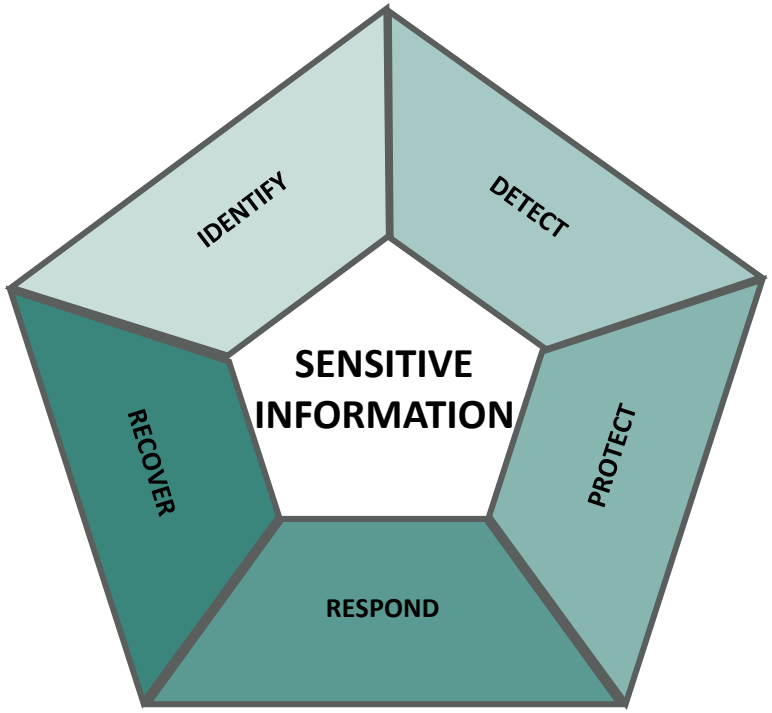
CYBERSECURITY IS A PROGRAM.

Compliance demands careful coordination of law, policy and technology.

Five Key Pillars of an Effective, Holistic Cybersecurity Program

Aid Organizations in Understanding Management of Cybersecurity Risk

www.nist.gov/cyberframework

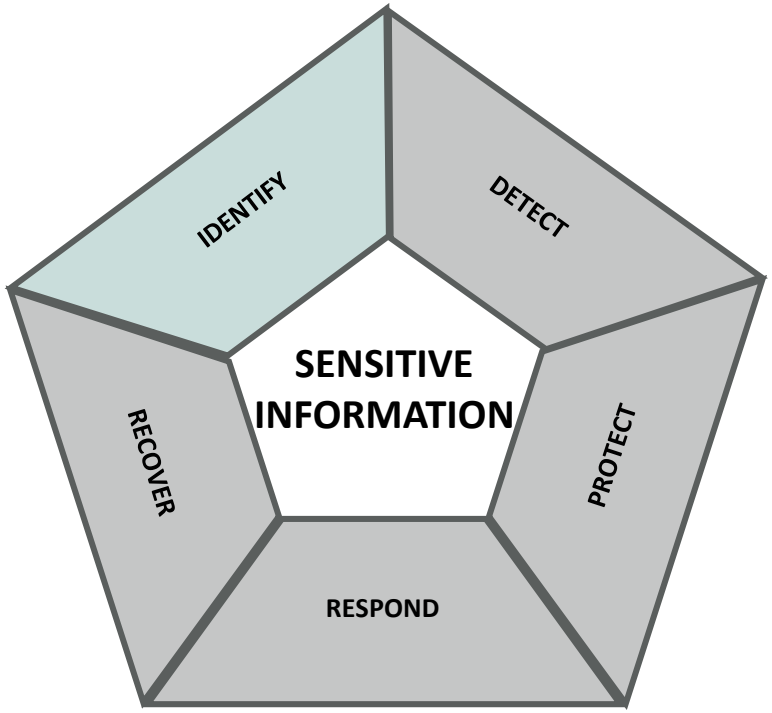


IDENTIFY.

Understand Risks to Systems, Assets, Data & Operations

Outcomes:

- Identifying physical and software assets to **establish an Asset Management program**
- Developing Cybersecurity policies to **define a Governance program**
- Defining a **Risk Management Strategy** for the organization

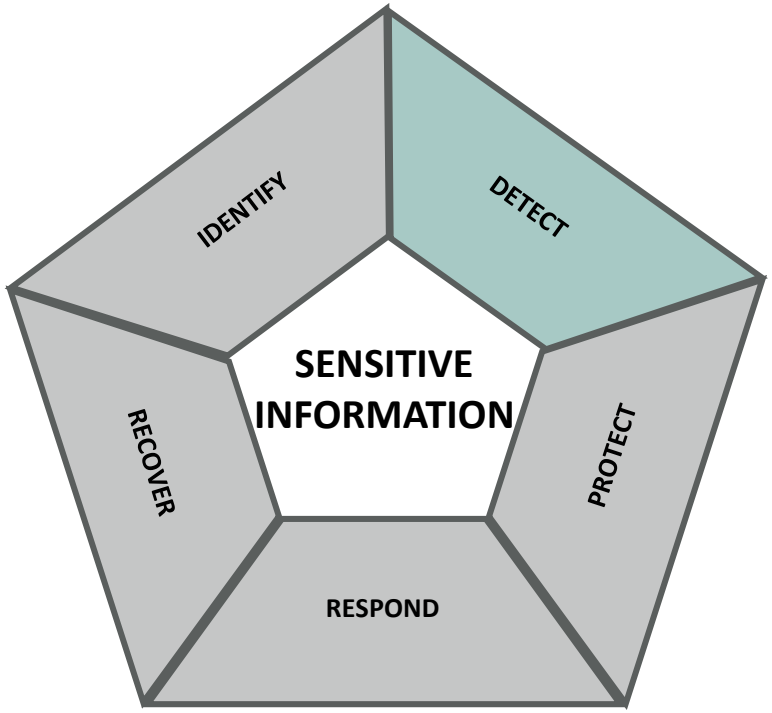


DETECT.

Real-Time Automated Identification of Cybersecurity Events

Outcomes:

- Implementing **Continuous Monitoring capabilities** to report Cybersecurity events
- Ensuring **Anomalies and Events are detected**, and their potential impact is understood
- **Verifying the effectiveness** of protective measures

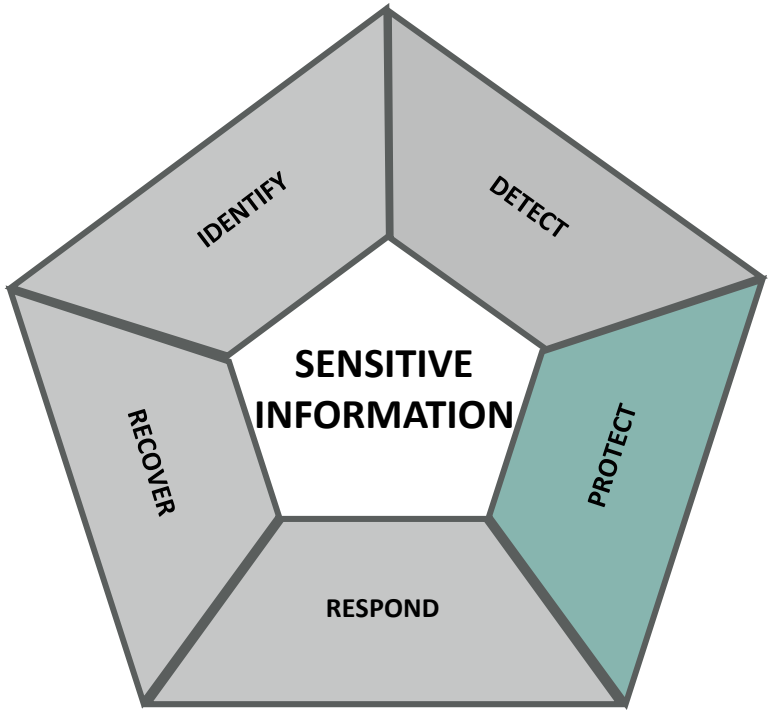


PROTECT.

Limit the Impact of Security Events & Safeguard Delivery of Critical Services

Outcomes:

- Establishing Data Security protection to **maintain confidentiality, integrity, and availability**
- Managing Protective Technology to **ensure the security and resilience of systems**
- Empowering staff within the organization through **Awareness and Training**

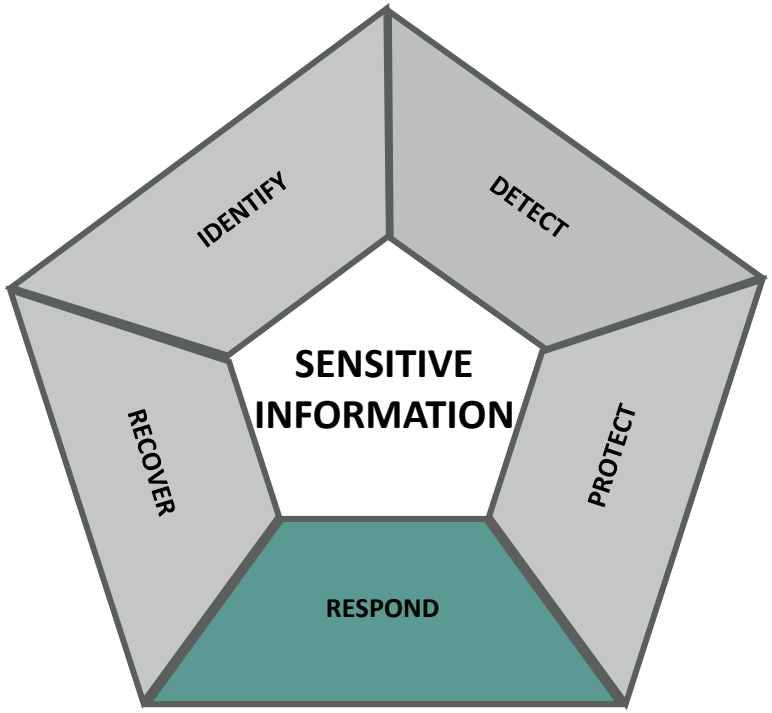


RESPOND.

Coordinated and Effective Responses to Detected Cybersecurity Incidents

Outcomes:

- Ensuring **Response Planning processes are executed** during and after an incident
- Managing **Communications** during and after an event
- **Analyzing effectiveness** of response activities

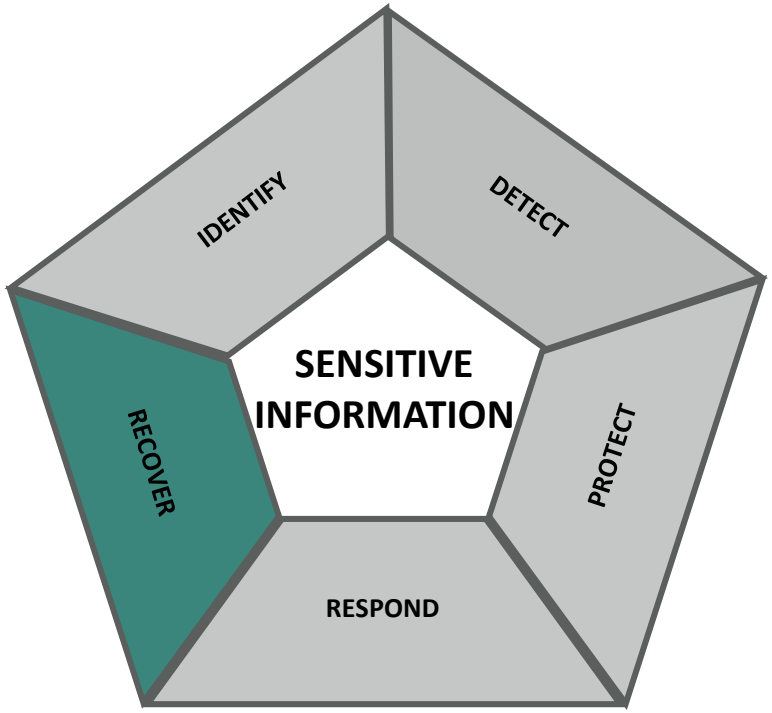


RECOVER.

Execute Plans for Resilience and Restoration of Services Impaired During Cybersecurity Incidents

Outcomes:

- Ensuring the organization implements **Recovery Planning** processes and procedures
- **Restoring Operations** after stability of Services has been tested and assured
- Implementing improvements based on L**essons Learned**



THE RISKS ARE REAL.

DoD Inspector General has Heightened Audit and Enforcement Standards

Failure to Protect CUI will have Real Consequences:

- “Stop Work” Order until Compliance is Achieved
- Termination for Default
- Debarment from other Federal Contracts
- Reputational Risk
- Financial Penalties
- Exposure to Damages Claims