National Institute of Allergy and Infectious Diseases

34th Annual FIRST Conference

Creating an Information Security/Information Assurance Program – Lessons Learned

Kenneth Grossman

NIAID Information Security Officer

Department of Health and Human Services/National Institutes of Health

29 June 2022

NIAID

National Institute of Allergy and Infectious Diseases

BIO

- NIAID Information Security Officer, 6/2006-Present
  - Established the first Information Security/Information Assurance Program for NIAID
- Information Security Specialist with FedCIRC/US-CERT, 1/2000-5/2006
  - Founding member of US-CERT
    - Part of team that established early SOPs and workflow
    - Part of team that established SOPs for US-CERT to interoperate with other parts of IAIP Directorate
  - Oversaw FedCIRC SOC
- FSS Information System Security Manager 7/1989-12/1999
  - Established the first Information Security/Information Assurance Program for GSA/FSS

Your organization’s mission

- Understanding of your organization’s mission
  - Public/Government
  - Private Industry
    - Banking
    - Financial
    - Manufacturing
  - Health Care
  - Academic/Research
- Do you conduct business in multiple countries?
- How does Information Security/Information Assurance play a role in fulfilling it.
  - How do you enable mission fulfillment

NIH National Institute of Allergy and Infectious Diseases

NIAID

Scope of your responsibilities.

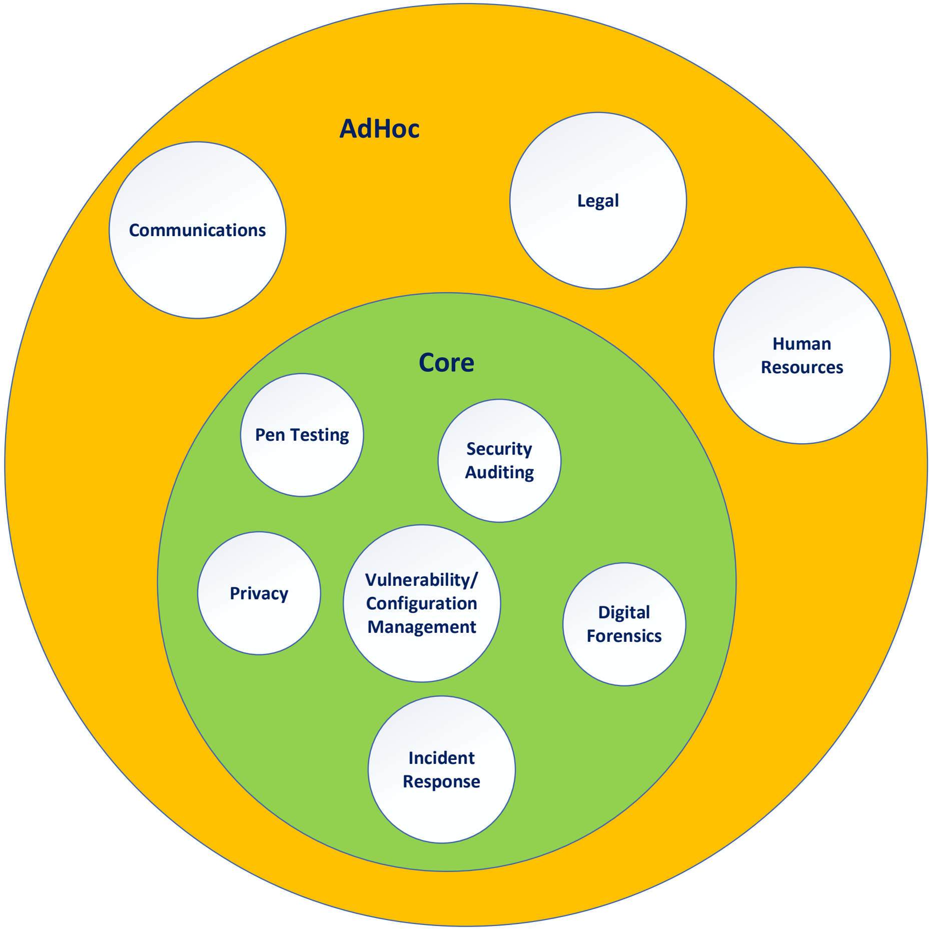
- What is the boundary of your responsibilities
  - Organization-wide
    - If international company, all countries vs. specific countries
  - Division-wide
  - Office-wide

Nature of your Information Security/Information Assurance team.

- Formal
  - Will it be standing group that is located together
- Virtual
  - Will the team be geographically dispersed
- Combination of both

National Institute of Allergy and Infectious Diseases

Makeup of your Information Security/Information Assurance team



National Institute of Allergy and Infectious Diseases

Who are your customers

- Know who your customers are
- Internal Customers
  - Could be your Office of the Chief Information Officer group
  - Could be your entire company personnel
- External Customers
  - Could be contractors
  - Could be other organizations with whom your organization has relationships

Organizational Politics

- Need to know organizational structure (who reports to who)
- Which parts of the organization have more clout within the organization as a whole

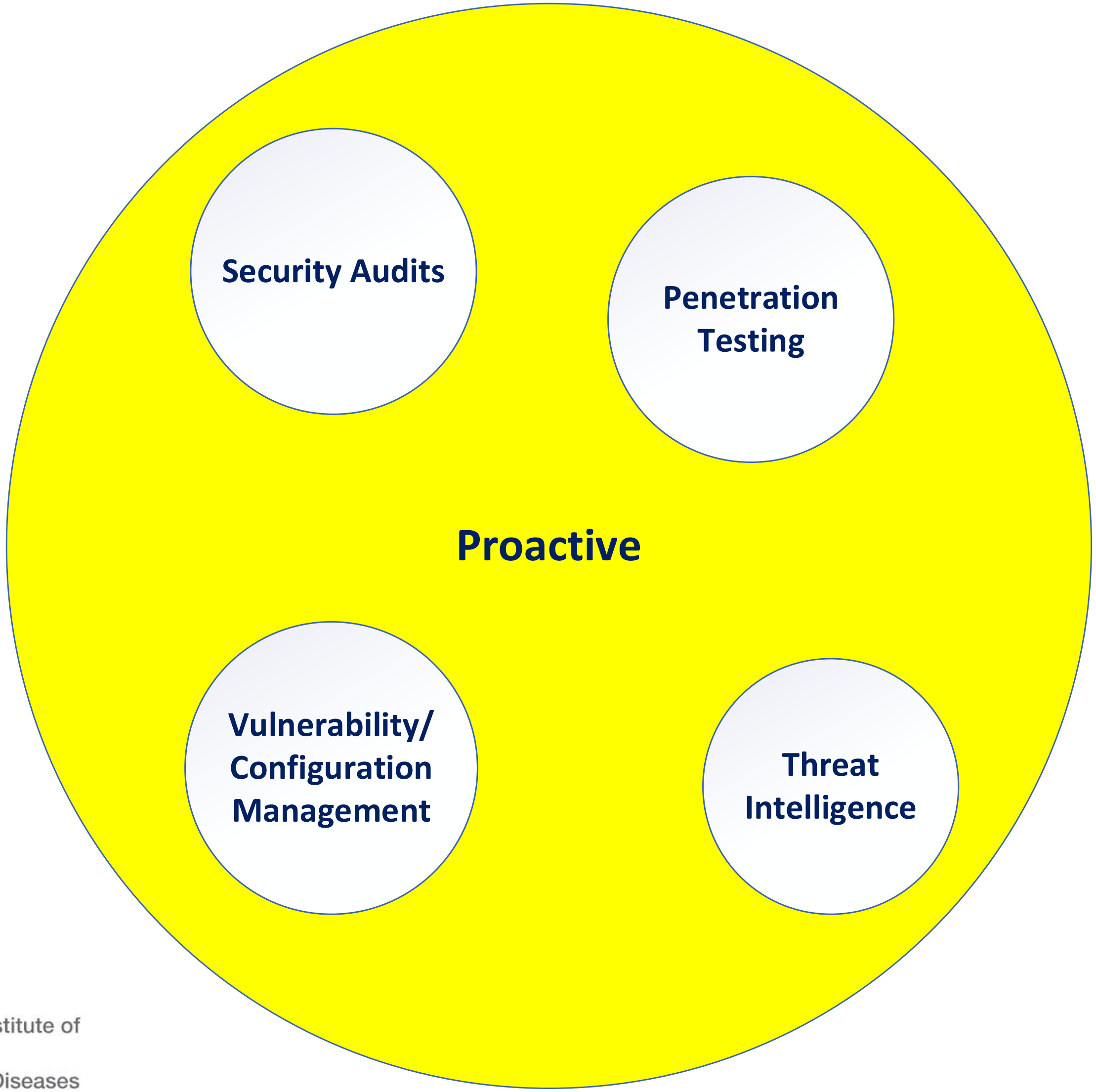
Regulatory Compliance Requirements

- Health Care
  - Health Insurance Portability and Accountability Act of 1996 (US)
  - Health Information Technology for Economic and Clinical Health Act of 2009 (US)
  - Genetic Information Nondiscrimination Act of 2008 (US)
- Financial
  - Sarbanes-Oxley (US)
  - Payment Card Industry Security Standards (international)
- Privacy
  - Privacy Act of 1974 (US)
  - General Data Protection Regulation (EU)
- Government
  - Federal Information Security Modernization Act of 2014 (US)
  - Network and Information Security Directive (EU)
  - Cybersecurity Act (EU)

Organizational Dependencies

- Do you have any internal dependencies?
  - Internal Customer Service/Helpdesk
  - Server team
- Do you have any external dependencies?
  - Managed Security Services Provider
  - External forensic organization
  - Other parts of your organization which are not part of your groups scope

Required Capabilities for the Information Security/Information Assurance Program



Security Audits

Penetration Testing

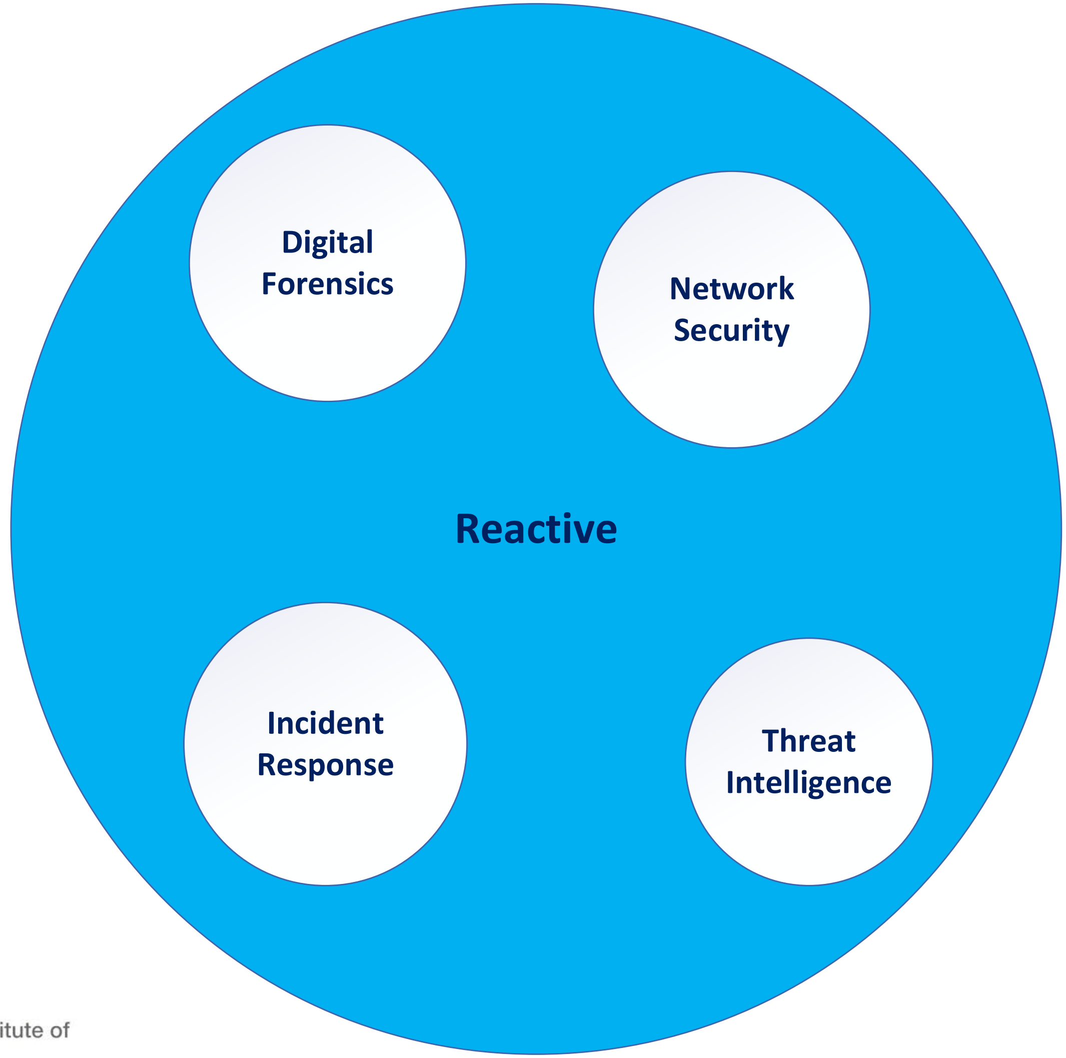
Proactive

Vulnerability/ Configuration Management

Threat Intelligence

National Institute of Allergy and Infectious Diseases

Required Capabilities for the Information Security/Information Assurance Program



National Institute of Allergy and Infectious Diseases

NIAID

?

Contact Information

- Ken Grossman
- E-mail: Kenneth.Grossman@nih.gov
- Phone: 1-240-627-3747