IT Infrastructure and Security
January 13, 2017

Andrea T. Norris, M.B.A.
Director, Center for Information Technology
and
NIH Chief Information Officer
Risk
Confidentiality
Integrity
Availability
Privacy
Security

Value
Open Environment
for
Research
Collaboration, and
Clinical Care

Life & Safety
Loss of Personal Identifiable or Personal Health Information
Research Data Integrity
Financial Stewardship
Administration and Operations
Federal Laws, Policies, and Standards

- Identify
- Protect
- Detect
- Respond
- Recover

...FISMA...
...HIPAA...
...Privacy Act...
...HITECH...
NIH Security Program

- Family of policies covering security controls consistent with federal laws and regulations, NIST guidance, and industry best practices

- Three annual independent audits review management of information systems
- Annual NIH review of IT and security controls

- Annual training for all staff and specialized training for key roles
- Periodic safe security practices and tips distributed NIH-wide

- Prepare for, detect, and contain information security incidents
- Investigate and coordinate recovery from information security incidents

- Inventory of NIH applications and general support systems (manual)
- Inventory of devices and equipment connecting to the network (automated)

- Processes and tools to discover, assess, and remediate security vulnerabilities
- Trusted penetration testing to independently assess the security of our systems

- Processes and tools to provide 24/7 situational awareness and security status of devices connecting to the network
Clinical Center Technology Environment

- **Electronic Health Record System**
  - Clinical Research Information System (CRIS), Allscripts Sunrise Clinical Manager

- **Clinical Research Data and Analytics**
  - Biomedical Translational Research Information System (BTRIS)

- **70+ Commercial and Custom Applications Supporting Clinical Care and Clinical Research**

- **Complex IT Infrastructure**
  - On Campus Data Centers Housing 750+ servers
  - 5,000 Laptops, Desktops and Mobile Devices
  - 900 Clinical Workstations
Multi-Dimensional Approach

CROSS-LAYER CAPABILITIES & SERVICES

- Vulnerability Scanning
- Continuous Monitoring
- Intelligence Analysis
- Penetration Testing
- Threat Detection

<table>
<thead>
<tr>
<th>Device</th>
<th>Data</th>
<th>Applications</th>
<th>Network</th>
<th>Perimeter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>Data Loss Prevention</td>
<td>Vulnerability Scanning</td>
<td>Firewalls</td>
<td>Firewalls</td>
</tr>
<tr>
<td>Encryption</td>
<td>Data Backups</td>
<td>Patch Management Tools</td>
<td>Identity and Authentication</td>
<td>Intrusion Detection/Prevention Systems</td>
</tr>
<tr>
<td></td>
<td>Access Controls</td>
<td>Access Controls</td>
<td>Network</td>
<td>Mail &amp; SPAM Security Filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Threat/Vulnerability Detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network Segmentation</td>
<td></td>
</tr>
</tbody>
</table>
Clinical Center Security Program

- Security integrated into IT management and governance processes
- Strong authentication and role-based access controls
- Data encryption and data loss prevention in progress
- Layered network security controls
- Frequent audits and assessments
Opportunities

• Real time visibility and understanding of systems and data assets

• Speed and agility to address known risk areas
  – Critical vulnerabilities in commercial and custom applications
  – End-of-life platforms and aging infrastructure
  – Remediation of penetration test findings

• Broader implementation of advanced security technologies to prevent and protect

• New approaches to meet demands for secure high availability, high quality IT services
Life & Safety

Loss of Personal Identifiable or Personal Health Information
Research Data Integrity
Financial Stewardship
Administration and Operations