## Cyber Incident Response Team

**Description**
The Cyber Incident Response Team responds to crises or urgent situations within the pertinent cyber domain to address, manage, and mitigate immediate and potential threats.

**Resource Category**
Cybersecurity

**Resource Kind**
Team

**Overall Function**
The Cyber Incident Response Team:
1. Investigates and analyzes all relevant cyber and network activities related to the crisis situation with the purpose of achieving the speediest recovery of the impacted critical infrastructure service.
2. Uses mitigation, preparedness, response, and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security.
3. Documents all steps and actions taken during the operations and develops Incident Action Reports (IAR).

**Composition and Ordering Specifications**
1. Discuss logistics for deploying this team, such as security, lodging, transportation, and meals, prior to deployment.
2. Teams work up to 12 hours per shift, are self-sustainable for 72 hours, and are deployable for up to 14 days.
3. The requestor may need to order multiple teams to provide 24-hour coverage.
4. A single source entity may constitute the entire team.
5. The requestor should specify if the personnel should have training and experience with specific software applications, hardware, and equipment.

<table>
<thead>
<tr>
<th>Resource Types</th>
<th>Type 1</th>
<th>No Type 2</th>
<th>No Type 3</th>
<th>No Type 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
<td><strong>Metric/Measure</strong></td>
<td><strong>Capability</strong></td>
<td><strong>Personnel</strong></td>
<td><strong>Personnel</strong></td>
</tr>
<tr>
<td>Personnel</td>
<td>Per team</td>
<td>Total</td>
<td>15</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td>NOTES:</td>
<td>Not Specified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td>Per team</td>
<td>Management and oversight</td>
<td>2 – National Incident Management System (NIMS) Type 1 Cyber Incident Responder</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td>NOTES:</td>
<td>Not Specified</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Resource Typing Definition for Cybersecurity

<table>
<thead>
<tr>
<th>RESOURCE TYPES</th>
<th>TYPE 1</th>
<th>NO TYPE 2</th>
<th>NO TYPE 3</th>
<th>NO TYPE 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMPONENT</strong></td>
<td><strong>METRIC/MEASURE</strong></td>
<td><strong>CAPABILITY</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Personnel      | Per team | Support | 1 – NIMS Type 2 Cyber Incident Responder  
3 – NIMS Type 1 Computer Network Defense (CND) Analyst  
1 – NIMS Type 1 CND Infrastructure Support Specialist  
1 – NIMS Type 2 CND Infrastructure Support Specialist  
1 – NIMS Type 1 Database Administration Specialist  
1 – NIMS Type 1 Digital Forensics Specialist  
1 – NIMS Type 2 Digital Forensics Specialist  
1 – Voice Communications Operator  
1 – System Administrator  
2 – Network Administrator | Not Applicable | Not Applicable | Not Applicable |           |
| Equipment      | Per team | Operations Equipment | 13 – Laptops with wireless internet card and programs for creation of documents, spreadsheets, and databases  
2 – Laptops with a digital forensics tool suite  
2 – Write-block hardware devices  
2 – Devices capable of live memory capture | Not Applicable | Not Applicable | Not Applicable |           |

**NOTES:**
1. All members of the team should hold an active security clearance.
2. Any use of the term “forensics” is descriptive of a skill or capability and does not imply a law enforcement role.
3. The Voice Communications Operator, System Administrator, and Network Administrator are not NIMS typed support positions.

1. Team may need additional equipment and supplies for small local area network interfaces to tactical outbound communications.
2. An understanding of asset information including operating systems, key applications, incident response plans, organization charts, emergency contact lists, and hardware is essential prior to deploying team, to ensure team brings the appropriate tools.
3. Iterations of training deployments determine additional software and hardware items to conduct forensics, network analysis, and other supporting functions.
Resource Typing Definition for Cybersecurity

<table>
<thead>
<tr>
<th>RESOURCE TYPES</th>
<th>TYPE 1</th>
<th>NO TYPE 2</th>
<th>NO TYPE 3</th>
<th>NO TYPE 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPONENT</td>
<td>METRIC/MEASURE</td>
<td>CAPABILITY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment</td>
<td>Per team</td>
<td>Communications</td>
<td>15 – Cell phones</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 – Satellite phone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not Applicable</td>
<td></td>
</tr>
</tbody>
</table>

NOTES: Not Specified

COMMENTS

The requestor provides support to the team, such as security, fuel, and power for recharging phones, computers, and other rechargeable devices.

REFERENCES

1. FEMA, NIMS 509-13: CND Analyst
2. FEMA, NIMS 509-13: CND Infrastructure Support Specialist
3. FEMA, NIMS 509-13: Cyber Incident Responder
4. FEMA, NIMS 509-13: Database Administration Specialist
5. FEMA, NIMS 509-13: Digital Forensic Specialist

NOTE

Nationally typed resources represent the minimum criteria for the associated component and capability.