# Vulnerabilities Across Campus Groups

<table>
<thead>
<tr>
<th>Persons of interest</th>
<th>Personnel Examples</th>
<th>Information Types Provided</th>
<th>Unique Vulnerabilities</th>
<th>Shared Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Expertise:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Individuals with expertise in fields or research on projects that have implications or direct applications for military or economic advantage | • PIs  
• Other project personnel  
• Faculty members  
• Graduate students  
• Research partnerships/private industry partners | - Information concerning specific project  
- Service or assistance  
- Inadvertent “clues” about funded projects or research findings  
- Access or clues concerning obtaining access | - Eager to talk about research  
- Regularly receive unsolicited contacts  
- Collaboration valued and often requested  
- Frequent travel to present research | - Face limited:  
• Salaries or Funding  
• Opportunities  
• Time  
• Understanding of Threat  
• Situational Awareness |
| **Access:**         |                   |                           |                        |                       |
| Individuals with privileged access to high-value or sensitive areas or items (labs, equipment, materials, substances, hard/software) | • PIs, project personnel, grad/undergrad students  
• Facility Security Officers or managers  
• Administrative staff  
• Information Systems staff  
• Cleaning crews | - Insider knowledge of access to spaces, items, persons  
- Insights to types of activities occurring in location  
- Understanding of work schedules and daily routines | - May become desensitized to security protocols due to everyday access  
- Hard to spot suspicious “insider threat” activities from legitimate, routine ones | - Desire to feel:  
• Important  
• Respected  
• Appreciated  
• Fulfilled  
• Engaged  
• Challenged  
• Connected |
| **Oversight:**      |                   |                           |                        |                       |
| Individuals with extensive knowledge of university projects and operations and having influence to make or impact institutional policy. | • Executive policy-makers  
• Department Heads and Deans  
• Empowered Officials  
• Technology Transfer  
• Compliance personnel  
• Information Security Officer | - Broader, more cohesive understanding of various activities occurring across campus  
- Position and power to influence institutional policies and upper-management connections | - Focused on increasing research profile rather than risk profile  
- More likely to advocate for or support foreign collaborations to improve university prestige  
- Susceptible to appeals to ego | - Unaware of personal vulnerabilities and methods of exploitation  
- Disinclined to adopt “zero trust” mentality. |
| **Support:**        |                   |                           |                        |                       |
| Individuals with insider knowledge about university employees and/or business functions. | • Human Resources  
• Administrative Assistants  
• Student and Scholar Services  
• Financial Aid | - Private personnel information (salary, resumes, visas, medical records, conflicts of interest, etc.)  
- Faculty coursework, schedules, contacts, etc. | - Able to ‘fly under the radar’ and avoid scrutiny of actions or behavior.  
- More likely to become disgruntled with lack of appreciation or recognition. | - |