



National Counterintelligence  
and Security Center

# SECURE INNOVATION

## INVESTORS SUMMARY



### KNOW THE THREATS

- People are a business' greatest asset but, in some cases, they can pose an insider risk
- Weak IT protocols can provide an easy way for your portfolio companies to be exploited
- Your portfolio companies' assets could be stolen via physical access
- Adversarial government actors can operate more easily overseas than in the U.S.
- Investment can be used to gain access to, and influence over, your portfolio companies
- International expansion exposes businesses to jurisdictional risk from foreign laws and business practices
- Vulnerable or malicious suppliers could compromise your profits

### PRE-INVESTMENT

- Does the company have any investors that pose significant risks?
- Could the involvement of other investors inhibit future fundraising or sale of the company because of legal, ethical, or compliance issues?



### SECURE ENVIRONMENT

- Is security owned and discussed at the Board level?
- Has the company identified its most valuable assets?
- Is security included in the company's risk register?
- Are security measures centered around the company's critical assets?

The information contained in this document is accurate on the date it was created and is intended as general guidance only. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies, or procedures and consult with independent experts. To the fullest extent permitted by law, NCSC accepts no liability whatsoever for any loss or damage incurred or arising because of any error or omission in the guidance or arising from any person acting, relying upon, or otherwise using this guidance. References in this product to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the Intelligence Community.





### SECURE PRODUCTS

- Has the company built security into their product(s) from the beginning?
- Does the company have a strategy to identify and manage their IP?



### SECURE PARTNERSHIPS

- Does the company conduct due diligence on all prospective partners – investors, suppliers and collaborators?
- Has the company limited the data, information, and knowledge it shares to only who/what is necessary and within its risk tolerance?



### SECURE GROWTH

#### Expand safely into new markets

- Has the company put in place proportionate and effective security procedures for any international travel?
- Is the company compliant with U.S. export laws and any other international export regulations that may apply?
- Is the company aware of local laws in countries into which they are expanding, and how those laws could affect the business?

#### Security for a growing team

- Has the company put in place pre-employment screening processes for all recruits?
- Does the company provide security training for all staff, including upon onboarding?

#### Prepare for security incidents

- Has the company established and tested an incident management plan?
- Does the company detect and investigate unexpected behaviors in IT and staff?

