|  |
| --- |
|  |
| Robert J. Smith, III 1827 University Avenue  Charlottesville, Virginia 22904  Email: erz8ep@virginia.edu |

University of Virginia: Cyber Due Diligence For Defense Research Lab Acquisition



Table of Contents

Executive Summary3

Report5

Regulations Governing Universities5

Regulations Governing Defense Contractors6

Proof of Compliance to Insurer7

Plan: Cybersecurity Due Diligence Team7

Plan: Initial Assessment8

Plan: Independent Review9

Plan: Financial Impact of Findings on Negotiations10

Conclusions11

Recommendations12

References13

I

## Executive Summary

## Overview

## The University of Virginia is positioned to acquire a robotics and weapons systems research and testing business (Easy Rider Corp.) with a significant volume of government contracts. Grant funds and donations from alumni and partner donors supported the acquisition offer. Our legal team has met with counsel for Easy Rider Corp. to commence the bidding process and obtained consent to proceed. In the interest of an active pre-acquisition phase, counsel asked us to limit our review of third-party risk management related to the federal contracts; Easy Rider LLC works with the appropriate federal resources to maintain compliance with defense-related regulations and will furnish the most recent reports. With our scope of investigation thus decreased, we both agree to a 120-day due diligence period.

## Purpose of Report

## This study is necessary guidance for navigating due diligence of cybersecurity and information resources that the acquisition will bring into the University’s scope of governance. The University’s due diligence efforts are compulsory for several reasons:

* Cybersecurity due diligence is a required stipulation in the due diligence checklist agreed to by the parties;
* The University’s cybersecurity insurance requires all University departments and assets to conform to its established framework; and
* The University must identify security risks and report them to the insurer to meet policy compliance.

## The due diligence plan of action also strategically reduces risks that might face the University:

* Differences in GRC styles between the University and Easy Rider Corp. necessitate evaluation; and
* Uncovered or undisclosed breaches will require additional legal guidance and may jeopardize the success of the acquisition.

**Regulatory Requirements**

The acquisition report provides layers of detail describing critical aspects of the University’s due diligence process that involve federal regulations. Compliance with these regulations also impacts the University’s insurability against cybersecurity incidents.

**University Regulations** – The Gramm-Leach-Bliley Act of 1999 (GLBA) requires the University to protect certain data sets, and the University maintains a version of NIST 800-171 per guidance from the United States Department of Education. Understanding these requirements will help the University map to other requirements inherited by acquisition of Easy Rider, Inc.

**Regulations for Defense Contractors** – Cybersecurity protections are a specific requirement of Easy Rider, Inc.’s defense research contracts. As a defense contractor, the organization must conduct self-assessments in accordance with the Defense Federal Acquisition Regulation Supplement (DFARS); the methodologies and frameworks carried in DFARS is entirely new to the University.

## Cyber Due Diligence of Defense Research Lab Acquisition

## The parties arrived at a 120-day due-diligence period due to the complexities of mapping the University of Virginia’s framework to meet the requirements of Easy Rider, Inc. (“the defense research lab”). Initial negotiations involved a discussion of retaining current defense research lab employees vital to the continuity of existing projects. The parties deemed this necessary due in part to the length of certain contracts; with no specific conclusion date, the parties could not schedule an acquisition timeline based on contract satisfaction.

## This report provides background on the University’s cybersecurity responsibilities under federal regulations and highlights the different regulatory rules for defense contractors. The contrast will serve to inform internal discussions of feasibility of the acquisition and also provide intel relevant to further negotiations over the terms of any agreement.

## Regulations Governing Universities

## The Gramm-Leach-Bliley Act of 1999 (GLBA) only requires colleges and universities to make efforts to protect student financial data, avoiding specific recommendations as to frameworks. The United States Department of Education provides guidance to institutions on higher education and recommends adherence to NIST 800-171, a framework of 110 different security controls. The University of Virginia heavily invested in its cybersecurity framework due to its organization as a public university and its dedication to protecting student information and is in full compliance with all controls prescribed by NIST 800-171. Consequently, the University falls into partial compliance with federal regulations governing Covered Defense Information; additional certification would allow the University to handle Controlled Unclassified Information (CUI) such as research and development data for Department of Defense contracts [1].

## Regulations Governing Defense Contractors

## In November 2020, new regulations subjected defense contractors in the United States to additional requirements on top of full NIST 800-171 compliance. Contractors must conform to the Cybersecurity Maturity Model Certification (CMMC) and a DoD Assessment Methodology. CMMC is in a five-year rollout plan, and the current regulation, released in November 2021, is CMMC 2.0. The Defense Federal Acquisition Regulation Supplement (DFARS), under DFARS clause 252.204-7019, stipulates that organizations entering into new contracts after November 30, 2020 must adhere to the DoD Assessment Methodology prior to final agreement [2].

## The University, already in full compliance of NIST 800-171, will be subject to CMMC Level Three upon acquisition. The CMMC framework stipulates that third-party assessment organizations will perform all cybersecurity assessments. The Office of the Secretary of Defense and the Military Services and Department determine the eligibility of such organizations [3].

## The DoD Assessment Methodology requires the contractor to submit to DoD inspections and provide access to facilities, systems, and personnel for a medium or high NIST 800-171 DoD Assessment. The University, in conjunction with the University of Virginia CISO and cybersecurity team, will need to facilitate access for such assessments which occur no more than every three years. The requirement does not apply to contracts inherited by the University through the proposed acquisition. The assessment process provides for summary level scoring. The University is responsible for submitting scoring by encrypted email. The DoD sends assessment scoring to the University, which has the opportunity to rebut within 14 business days before the DoD publishes the scores on the Supplier Performance Risk System (SPRS) interface; authorized individuals at the University will have access to the SPRS to view summary scores following publication [3].

## Proof of Compliance to Insurer

## The University actively holds a cybersecurity insurance policy covering the risk of a data breach of protected information for students, faculty, and administration. The Chief Financial Officer (CFO) is responsible for purchasing insurance policies and works with the Chief Information Security Officer (CISO) to determine the extent of cybersecurity insurance policies [5]. The CISO will need to discuss changes in architecture, data handling, and access with the current insurance provider to determine which policy additions are appropriate after this acquisition. The University is not required to purchase cybersecurity insurance, and the acquisition will not change that status, but continuation of the University’s cybersecurity policies include a plan for insuring against security breaches.

## Plan: Cybersecurity Due Diligence Team

## The parties agree to a compliant risk assessment of the defense research lab necessitating the formation of an action team at the University. The Due Diligence Team of the University shall consist of the CISO, the Deputy CISO, the Director of Information Security Engineering, the Directory of Information Security Operations, the Director of IT Compliance, and the Director of IT Policy and Outreach. A combination of expertise on system architecture, incident response, compliance, and information security policies will best inform the due diligence process for the proposed acquisition [4]. The Due Diligence Team will coordinate with the CFO on necessary changes to the cybersecurity insurance plans.

## The Due Diligence Team will formalize a reporting standard for assessing risk and be familiar with the University’s risk tolerance. The reporting standard should also conform to a common assessment metric while assessing the acquisition target [6].

## Plan: Initial Assessment

## The maturity level of the target organization is critical in establishing a full understanding of risk. How it views cybersecurity will inform its risks. The Due Diligence Team will review public information about known data breaches involving the target. The Team will also request:

## All cybersecurity risk assessment reports and relevant data;

## Complete documentation of company cybersecurity policies, processes, and procedures;

## Documentation of any changes to cybersecurity policies, processes, and procedures;

## Review of the incident response policy;

## Recent audit reports and relevant data.

## The acquisition target will provide an inventory of the following items that will constitute its Digital Assets:

## All related IP addresses;

## All active and inactive users;

## All network devices;

## All physical and virtual machines;

## All workstations;

## Data storage locations;

## Service providers (cloud, security); and

## Application stack [6].

## The combined results of the initial assessment will help establish additional momentum to carry the transaction forward into a phase of deeper analysis. If the Due Diligence Team encounters issues in its early assessment phase, it will work with the acquisition target’s cybersecurity team to review further.

## Plan: Independent Review

## Barring any red flags that could jeopardize the acquisition negotiations and render transaction unsustainable, the Due Diligence Team should engage in additional systems analysis through several methods:

## Obtain and review available penetration test reports;

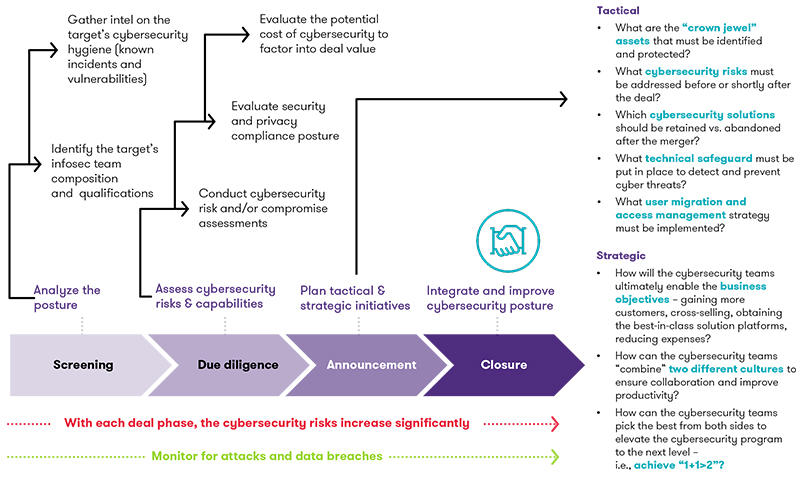
## Conduct deep web research for any sensitive data related to the business; and

## Conduct network monitoring.

## If penetration test reports are not recent or contain potential issues, the Due Diligence Team may choose to hire a third-party penetration tester to appropriately test the target’s systems [6].

## Plan: Financial Impact of Findings on Negotiations

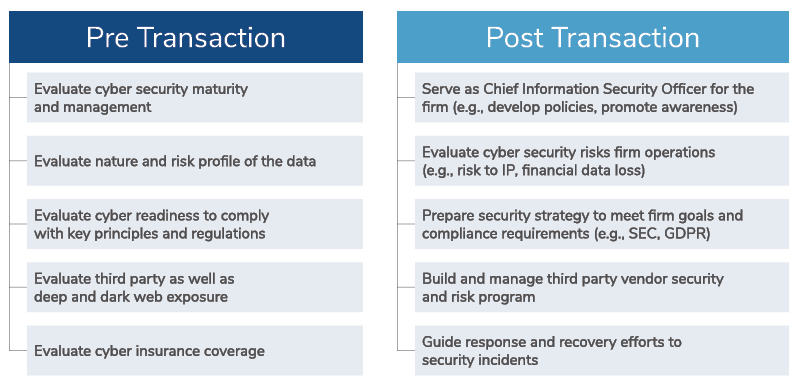
## Initial discussions of the acquisition target’s systems indicate that equipment upgrades will not likely be necessary after final execution of the transaction. Barring any discovery of breaches or other significant incidents, the Due Diligence Team should expect to encounter costs from adding staff to the University to accommodate inter-administration and inter-student body resources, any increases in cybersecurity insurance, and security weaknesses expected during the integration phase after the execution of the acquisition agreement [6].



## Sample plan with additional insights on objectives [7].

## Conclusion

## The University’s proactive pursuit of mature cybersecurity policies and practices make this acquisition effort simpler. The University already maintains a full NIST 800-171 security framework and would not face prohibitive costs or implementation timelines by completing the acquisition. The transition will involve additional steps by the University’s CISO and cybersecurity team. The University will need to reassess its posture and update its security policies to meet new demands on its compliance requirements.



## Sample overview of transition strategy before and after the execution of the transaction [8].

## Recommendations

After preliminary and follow-up discussions with the cybersecurity team and executives at the defense research lab, and after consulting with the University’s CISO, I recommend that the University enter into the initial risk assessment phase. I also recommend that the University prepare to hire supporting staff as well as existing employees of the lab to ease the transition. The University should offer essential lab employees continued employment following the transition and facilitate training for vacated positions as necessary. Adoption of this plan will protect the University from unforeseen risks and will allow the University to adopt the research lab into its fold of services without undue financial harm.

References

[1] Totem Technologies. (2022). *Cybersecurity expectations for higher educational institutions*. Totem Technologies. <https://www.totem.tech/cybersecurity-requirements-for-colleges-and-universities/>

[2] Brook, C. (2020, November 10). *New government contractor cybersecurity requirements loom*. Digital Guardian. <https://digitalguardian.com/blog/new-government-contractor-cybersecurity-requirements-loom>

[3] United States General Services Administration. (2020, October 19). *252.204-7020 NIST SP 800-171 DoD assessment requirements*. United States General Services Administration. <https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171-dod-assessment-requirements.>

[4] University of Virginia. (2022). *University information security (InfoSec)*. University of Virginia. <https://security.virginia.edu/about-university-information-security>

[5] Snyder, J. (2022, March 14). *What higher education institutions need to know about cyber insurance.* EdTech. <https://edtechmagazine.com/higher/article/2022/03/what-higher-education-institutions-need-know-about-cyber-insurance>

[6] Security Scorecard. (2021, June 30). *Cybersecurity due diligence in M&A*. Security Scorecard. <https://securityscorecard.com/blog/cybersecurity-due-diligence-in-m-a>

[7] Informational graph. (2021). Grant Thornton. <https://www.grantthornton.com/library/articles/advisory/2021/cybersecurity-in-ma-strategy.aspx>

[8] Informational graph. (2022). Kroll. <https://www.kroll.com/en/services/cyber-risk/assessments-testing/cybersecurity-due-diligence-ma>