Penn State Lawsuit Executive Summary

HRTec

Ian Mabon

9/29/23

**Executive Summary:**

This case against Penn State University submitted by Matthew Decker alleges Penn State disregarded the required security compliance for government contracts, failing to adhere to NIST and DFARS requirements for important CUI. Multiple executives involved in the IT department and Office of Information Security were aware of this noncompliance and continued to give ATO for contracts being worked on within the university. They did not submit the required System Security Plan or do a supplemental Plan of Actions and Milestones as well. This was all sparked by an incident in 2015 where the College of Engineering and College of Liberal Arts suffered a massive cyber-attack, prompting the university to hire the relator (Matthew Decker) to upgrade security and work on compliance for NIST. At first, he introduced the “Cavirin” software, which is a similar compliance software to what HRTec offers, but ultimately the software was unused or unable to help PSU reach full compliance. In addition to this, the university concluded their contract with Microsoft’s Box (FEDRamp compliant) in 2020 where they moved all their CUI to OneDrive, a noncompliant cloud storage service. The relator warned the university multiple times about their noncompliance issues, but they were unreceptive to his suggestions and proceeded to see what contracts they could still pursue without compliance. Their ATO was given to them by the Office of Information Security in the form of the university policy AD95, which was allegedly based off the NIST requirements, but did not address CUI nor the entire control family of NIST. The CISO, Richard Sparrow, used blank template documents in places where the university was noncompliant to submit the Supplier Performance Risk System, essentially “plugging the holes” in their report to still be given ATO. Matthew Decker is suing for damages toward the US government and personal compensation for bringing this issue to light.

**Notes:**

Compliance Issues

* 2015 cyber attack
* ARL was compliant because of relator’s efforts for DFARS compliance
* Cavirin compliance software introduced but not installed?
* PSU work day and Enterprise Resource Planning projects needed to be compliant with DFARS/NIST
* PSU missing SPRS entries
* Concluded contract with Box (FEDRamp compliant solution) in 2020 and went to OneDrive (not compliant)
* Penn State policy AD95 said it was based off of NIST requirements, but does not address CUI nor does it address the entire control family of NIST
* Started SSP two years too late
* Haven’t been compliant since 2018
* No worked was stopped even after finding out they were non compliant

Parties of Interest

* Matthew Decker vs Penn State

Matthew Decker

* Chief Information Officer for Penn State’s Applied Research Laboratory (ARL) since 2015
* Interim Vice Provost and CIO of Penn State itself in 2016

Safeguarding Covered Defense Information and Cyber Incident Reporting

* DFARS 252.204-7012
* Requires contractors like Penn State to provide “adequate security” for covered defense information that is processed, stored, created, or transmitted on its internal information systems

Controlled Unclassified Information (CUI)

* Information owned or created by the government that is sensitive, but not classified, such as technical data, patents, or information relating to the manufacture or acquisition of goods and services

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (NIST 800-171)

* All defense contractors must carry out Basic Assessments of their compliance with NIST SP 800-171 and submit their scores to the DoD as a condition of receiving a DoD contract
* 14 groups of security requirements (110 requirements in total)
  + Each requirement has a score of 1 point if followed
  + If not compliant, some are weighted higher than others in negative points
* No official audit for compliance for these requirements
  + Need to do self assessment
  + Self submit score for DoD contract to DoD’s Supplier Performance Risk System (SPRS)
* Any requirements not met have to be stated in a Plan of Actions and Milestones
  + Sets a timeline for compliance
  + Can be updated
* Must also submit System Security Plan
  + Details about security processes / hardware and software
* Failure to monitor NIST compliance is a violation of Section 3.3, Audit and Accountability

Penn State’s Compliance

* Huge security breach in College of Engineering and College of Liberal Arts
* Relator brought in to bring IT and cybersecurity environment to Applied Research Laboratory
  + Separate from Penn State
* Relator had no responsibility to bring Penn State’s research department with DFARS (security for defense information)
  + Asked to give an overview of compliance requirements and was named Interim CIO in December 2015

2015 - 2016

* Told Penn they needed to assess environments within College of Engineering
  + Had projects where DFARS applied
* Introduced Penn State to “Cavirin” a compliance software
* Penn State disregarded his suggestions concerning NIST compliance in the ERP implementation, which may have left more CUI exposed
* Many requirements were missing from SPRS test for compliance
  + Richard Sparrow became CISO and used templet documents (empty) to fill in each place they were missing a requirement
  + Knowingly false

2020

* Penn State moved CUI to Microsoft Office OneDrive in 2020, which was not compliant with NIST
* Tried to form group to offer assistance on DFARS compliance, but no one wanted to deal with it

2022

* Wanted NASA contract, but concerned about compliance with DFARS and CUI protection
* Penn State Policy AD95
  + Based upon NIST standards
  + Office of Information Security had authority to operate under this policy
* Never made a SSP for compliance and just began making one in June
* Vice President of Research created a “tiger team” to evaluate PSU’s compliance with DFARS
  + Relator and Mr. Crain didn’t tell the team about DFARS compliance
* All 20 contracts that were submitted were falsified

Charges

* Penn State knowingly presented or caused to be presented false or fraudulent claims for payment or approval, in violation of 31 U.S.C. § 3729(a)(1)(A)
* Government is entitled to monetary compensation for these violations
  + Relator gets attorney fees and reward for helping gov