

Coalfire Investigation Report

October 9, 2019

**FAEGRE BAKER
DANIELS**

Table of Contents

Introduction.....	1
Key Personnel.....	1
Findings of Fact	2
A. Prior Coalfire Engagement in 2015.....	3
1. Service Order.....	3
2. Rules of Engagement	3
3. Authorization.....	4
4. Summary Report	4
B. 2019 Selection of Coalfire.....	4
C. Planning & Documents	5
1. Service Order.....	6
2. Scoping Call.....	6
3. Kick-Off Call.....	7
4. Rules of Engagement	8
5. Authorization.....	10
6. Reporting to SCA Leadership	11
7. Legal Review.....	11
D. Testing.....	11
E. Arrest of Coalfire Employees.....	12
Analysis.....	12
A. Confusion Over the Parameters of Red Team Testing.....	12
1. Misunderstanding “Red Team” Techniques and Terminology.....	13
2. Ambiguous Terms within the Coalfire Agreement.....	13
3. Inconsistency Between the 2015 and 2019 Red Team Assessments	14
B. Lack of Oversight.....	15
C. Failure to Appreciate the Impact on Third Parties	15
D. The SCA’s Authority to Grant Coalfire Access to County Courthouses.....	16
Conclusions & Recommendations.....	17
A. Conclusions	17
B. Recommendations	18

Introduction

The Iowa Supreme Court has engaged Faegre Baker Daniels, LLP (“FaegreBD”) to investigate the State Court Administration’s (“SCA”) engagement of Coalfire Labs (“Coalfire”) and the related incidents that occurred at the Polk County and Dallas County courthouses. This report represents the factual findings, analysis, and recommendations from the investigation.

The investigation was led by Nick Klinefeldt and Paul Luehr of FaegreBD. FaegreBD is a global law firm with a substantial presence in the Midwest, including an office in Des Moines, Iowa. Nick Klinefeldt is a partner in FaegreBD’s Des Moines office and chairs the firm’s White Collar Defense and Internal Investigations group. He is the former U.S. Attorney for the Southern District of Iowa. Paul Luehr is a partner in FaegreBD’s Minneapolis office who chairs the firm’s Privacy and Cybersecurity group. He is a former federal prosecutor who also served as a national cybersecurity consultant, leading forensic investigations into large breaches (e.g. the Target and Yahoo! incidents) and overseeing security assessments and “Red Team” exercises. They were assisted in this investigation by Associates David Yoshimura, Kathryn Allen, Monika Sehic, and Adam Smith.

FaegreBD conducted this investigation over the course of approximately two weeks to provide a prompt reporting as directed by the Iowa Supreme Court. As part of the investigation, FaegreBD collected and reviewed numerous documents. The documents it collected and reviewed consisted of emails; electronic documents collected from shared drives, hard drives, and SharePoint sites; hard copy documents, such as notes; and, text messages. FaegreBD then conducted interviews of relevant witnesses from the SCA. In addition, FaegreBD reached out to Polk County and Dallas County Attorneys’ Offices, counsel for Coalfire, and counsel for the Coalfire employees who were arrested at the Dallas County courthouse. Both counsel for Coalfire and counsel for the Coalfire employees provided FaegreBD with helpful information, including statements and their versions of events. The Polk County and Dallas County Attorneys’ Offices did not provide FaegreBD with any information. Accordingly, this investigation did not include any information from law enforcement personnel or any law enforcement investigation.

Key Personnel

The key SCA personnel in this investigation are as follows:

Todd Nuccio, State Court Administrator (“Nuccio”)
Elaine Newell, Counsel to State Court Administrator (“Newell”)
Mark Headlee, IT Director (“Headlee”)
John Hoover, IT Manager (“Hoover”)
Andrew Shirley, Information Security Officer (“Shirley”)

Their reporting responsibilities are as such: Nuccio reports to the Chief Justice; both Newell and Headlee report directly to Nuccio; and, Hoover and Shirley both report to Headlee.

Findings of Fact

This matter involves advanced forms of cybersecurity assessments known as penetration (or “pen”) testing and “Red Teaming.” In both cases, cybersecurity experts employ a variety of the same techniques used by adversaries to gain access to a client’s computer data. Some experts have used the terms “pirates” versus “ninjas” to distinguish these forms of testing.¹ Pen testers (“pirates”) are also called “white hat” or “ethical hackers” and they often try to test as many different network vulnerabilities as possible by surveilling, probing, and attacking client systems using *online* techniques. Pen testers often work within a prescribed time period, with or without notice to the defending IT security team. Red Teams (“ninjas”) have one primary objective – “get in.” Sometimes considered a subset of pen testing, Red Teams typically take more time, provide little or no notice to the defending team, and try to enter computer networks using a combination of stealthy online or real-world *physical* techniques.

While most lay people may view cybersecurity purely as a networking issue, testing physical controls around data is widely considered a “best practice” by security experts like the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).² FaegreBD reviewed the sites of multiple national cybersecurity companies and found that they all offer Red Team services like those procured in this matter. Sophisticated corporations regularly employ Red Teams across the country, and we know that the federal government has often used Red Teams, especially in the military.³ We are not aware of what, if any, other state agencies have used Red Team assessments.

In this matter, the online techniques used to conduct a penetration test do not appear to be contested or controversial; therefore, our investigation focused on the types of *physical* actions taken by the Red Team assessors, particularly around county courthouses and judicial buildings.

¹ See K. Hayes, “Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues,” Rapid7 blog (June 23, 2016) at <https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/>

² The NIST Cybersecurity Framework describes the need to establish “Protections for Identity Management and Access Control within the organization including *physical* and remote access.” It also stresses the need to “verify the effectiveness of protective measures including network and *physical* activities.” See NIST CSF at <https://www.nist.gov/cyberframework/online-learning/five-functions>. Likewise, the CIS has stated, “Many attacks occur[] across the network, while others involve[] physical theft of laptops and other equipment holding sensitive information. ... The movement of data across network boundaries both electronically *and physically* must be carefully scrutinized to minimize its exposure to attackers. See CIS Control 14 - Controlled Access Based on the Need to Know at <https://www.cisecurity.org/controls/controlled-access-based-on-the-need-to-know/>

³ The Red Team concept grew out of the armed forces and defense industry, especially after 9/11 when the 2003 Defense Science Review Board recommended the expanded use of Red Teams to challenge conventional wisdom and expose vulnerable systems before they could be exploited by U.S. adversaries. See Defense Science Board Task Force, “The Role and Status of DoD Red Teaming Activities” (Sept. 2003), accessible at <https://fas.org/irp/agency/dod/dsb/redteam.pdf>

A. Prior Coalfire Engagement in 2015

The SCA initially engaged Coalfire to conduct testing of its network and facilities back in 2015. Headlee, then the Deputy IT Director, was in charge of overseeing this testing for the SCA. The Master Agreement with Coalfire, dated January 14, 2015, was signed by Headlee and listed Headlee as the client contact. There was no new Master Agreement signed in 2019. With some exceptions, the the other 2015 documents used similar language to the 2019 Coalfire documents.

1. Service Order

The service order for the 2015 testing was entitled, “Service Order for 2014 Red Team Penetration Testing.” It was actually dated August 18, 2014, but not signed until January 13, 2015. The SCA’s then-IT Director, Ken Bosier (“Bosier”), was the one who signed that document. In the 2015 service order, Coalfire described the type of “[p]hysical” testing it did as follows:

Using in-person pretexting, or by physically subverting your security controls, Coalfire staff will attempt to gain access to your physical network to plant devices that can be used to exploit vulnerabilities on your internal systems. This may include covertly deploying systems on your network that can be accessed remotely, or by “conveniently” leaving media infected with Trojans around your offices.

2. Rules of Engagement

The Coalfire Rules of Engagement, dated February 27, 2015/signed March 27, 2015, (“2015 ROE”) was signed by Headlee. There are a few important aspects of the 2015 ROE worth pointing out. First, the 2015 ROE limited testing to “normal business hours” defined as “8AM CST – 5PM CST.” Headlee explained that he changed this from the prior language in Mountain Time, because he only wanted the testing done during the SCA’s business hours.

Second, among the questions asked by Coalfire in the 2015 ROE section entitled, Information Required for the Physical Security Assessment, Headlee answered “Yes” to the following questions:

- Does Coalfire have permission to “tail-gate”, that is, attempt to gain physical access to your facilities by following employees into the building?
- Does Coalfire have permission to access all areas inside the building(s)?
- Does Coalfire have the permission to do non-destructive lock picking?

Third, the 2015 ROE also identified certain “Risks.” Those “Risks” included the following:

- Where the engagement includes testing physical security mechanisms, the penetration tester may utilize physical penetration testing techniques to gain access to facilities, sensitive information, networks or systems.

- Where the engagement includes testing physical security mechanisms, at no time during attempts to gain physical access will Coalfire destroy or be destructive to assets.
- Where the engagement includes testing physical security mechanisms, advanced notice will be provided with respect to any proposed target facilities.
- Physical Social Engineering/Destruction of Property/Physical Harm – Social engineering services may involve attempts to physically access subject facilities in order to gather sensitive documents and/or data and access the subject internal network for additional penetration testing activities. Such access will be attempted by subverting existing physical controls, but will not damage or destroy subject property in the process. Additionally, where physical harm is a possibility (e.g. armed personnel are protecting property and subject assets), Coalfire will make no attempts at physical access. For all such social engineering activities, a “get out of jail free” letter, which includes subject contact and Coalfire personnel IDs, will be presented in the event that Coalfire social engineers are “caught in the act”.

3. Authorization

The Penetration Testing Authorization (a.k.a. the “get out of jail free” letter), dated March 23, 2015, was signed by both Headlee and Bosier. It identified the Coalfire team member approved to do the testing, as well as contact numbers for Headlee and Bosier. In addition, it identified the “acceptable actions” as including:

- Gaining unauthorized access to restricted areas
- Social Engineering of personnel to gain elevated access
- Impersonations of Iowa Court Information Systems employees

This authorization did not specifically identify any actions that were unacceptable.

4. Summary Report

At the conclusion of the 2015 testing, Coalfire issued a Red Team Test Summary Report, prepared for Headlee, dated May 1, 2015. Coalfire also issued a Red Team Test Executive Summary, prepared for Headlee, dated July 15, 2015. While the full report goes into more detail, both reports identify that Coalfire assessors went into four county courthouses (Polk, Tama, Marshall, and Story) and attempted to enter the Judicial Building all seemingly during normal business hours. Headlee confirmed it was his understanding that – per his explicit instruction to Coalfire – its assessors only attempted to enter buildings during normal business hours.

B. 2019 Selection of Coalfire

The SCA engaged Coalfire again to conduct testing of its network and facilities in 2019. Sometime in mid-2018, Headlee tasked Shirley to be in charge of selecting a vendor to conduct penetration testing. Shirley reported that he was busy on other matters, so it took him awhile to

get quotes from vendors. On April 10, 2019, Shirley sent a request for quotes for “Red Team testing services” to potential vendors. With regard to physical penetration testing, Shirley described that the SCA “roughly needed” the following:

Physical Penetration Testing – Controlled areas

- a. Gaining access to controlled areas in our buildings, bypassing security controls
- b. Leaving infected media around the offices

On May 10, 2019, Shirley sent Headlee an email with an Informal Quote Selection form and Statements of Work (“SOW’s”) from three vendors: Coalfire; Protiviti; and, ConvergeOne/GreyCastle. Like the Coalfire SOW, the Protiviti and ConvergeOne/GreyCastle SOW’s both addressed physical penetration testing. The Protiviti SOW identified it under, “Social Engineering Assessment,” and stated it would include three physical locations. It also stated that “physical access may be attempted through the use of techniques such as ‘piggy-backing,’ striking up random conversation or flashing a driver’s license place of company badge or ID.” The ConvergeOne/GreyCastle SOW described the penetration testing as follows:

Using both Social Engineering tactics, tailgating, and other measures, ConvergeOne/Grey Security personnel will target to gain physical access to controlled areas as defined by Iowa Judicial Branch.

The ConvergeOne/GreyCastle SOW also stated that “[p]hysical [p]enetration” testing would occur at the “controlled areas” of four building identified by the SCA.

Out of the three firms that submitted proposals in 2019, the SCA selected Coalfire to once again conduct the penetration and Red Team testing. Shirley explained that the difference in quotes between the three was not significant. He also said that Coalfire had performed well in 2015, and he wanted to compare the 2015 Coalfire results with its 2019 findings. The approvals apparently required to engage Coalfire for this testing appears to have been Shirley, Headlee, and possibly a procurement officer. Nuccio stated he was not involved in the process to select Coalfire. Newell also stated she was not involved in the Coalfire in that process and did not review any of the documents beforehand. In fact, Newell explained she was not involved with the Coalfire testing until after it was over.

As part of Shirley’s selection of a vendor for the testing, Headlee provided Shirley with access to the reports from Coalfire’s 2015 testing. Shirley was not employed by SCA in 2015, and stated the only 2015 document he reviewed was the executive summary. However, the executive summary report still identified that Coalfire assessors went into four county courthouses (Polk, Tama, Marshall, and Story) and attempted to enter the Judicial Building all seemingly during normal business hours.

C. Planning & Documents

The planning for Coalfire’s testing occurred in the summer of 2019 and was governed by three documents from Coalfire: (1) the SOW or “Service Order”; (2) the “Penetration Test Rules

of Engagement” (“ROE”); and, (3) the “Social Engineering Authorization,” a.k.a. “get out of jail free” letter (“Authorization”). In addition, there were two conference calls that informed this process. There was one call described by participants as a “scoping” call that apparently took place at the beginning of the planning around April 17, 2019. Then, there was a “kick-off” call on August 14, 2019, where they discussed the Rules of Engagement.

1. Service Order

The Coalfire Service Order stated that Coalfire would perform “physical attacks” and described that testing as follows:

Physical attacks are those which require proximity to your facilities and typically include attempts to gain unauthorized access to your building(s) and, subsequently, your internal network assets. Due to proximity requirements, physical attacks may also include targeting your wireless infrastructure to attempt gaining unauthorized and persistent access to the internal network.

Physical Penetration Test targets your facilities/buildings/locations.

Number of location in scope: 3

Approach: Social engineering focused – limited technical physical approach

- Location 1: Polk Courthouse
- Location 2: Location within 20 miles
- Location 3: Location within 20 miles

- Attempt to physically gain internal network access
- Attempt to collect physical documentation at up to 3 locations
- Attempt to gain network access to facilitate persistent access

This document was dated, April 17, 2019. However, it was subsequently signed by Headlee on May 28, 2019.

2. Scoping Call

On April 17, 2019, there was a scoping call with Coalfire employees Joseph Neumann (“Neumann”), Principal responsible for penetration testing with Coalfire, Gil Urena, Coalfire Sales, and Shirley. According to an Affidavit from Neumann, that call included a discussion of physical testing and on it Shirley requested that physical testing and social engineering be performed on multiple courthouses in the state. Neumann stated that, on that call, they discussed both lock picking and tailgating as well as testing during the workday and after-hours testing, and that Shirley confirmed that all these activities were in scope. Shirley said he does not remember that specific call but remembered discussing physical testing after-hours at some point in the contracting process.

3. Kick-Off Call

Leading up to the second call, Coalfire sent Shirley and Headlee drafts of the ROE and Authorization on August 6, 2019, and highlighted a few items for Shirley's attention with respect to the ROE. The items highlighted by Coalfire included the scope of testing and a request for information. The scope of testing included a "[p]hysical security assessment" identified as follows:

- Attempt to gain physical documentation at three locations
 - Polk County Courthouse
 - 500 Mulberry Street, Des Moines, IA 50309
 - Warren County Courthouse
 - 2205 W. 2nd Avenue, Indianola, IA 50125
 - Dallas County Courthouse
 - 801 Court Street, Adel, IA 50003
- Focus on breaking in after-hours
- Talk you [sic] way in to area, limited physical bypass
- Attempt to physical gain internal network access
- Attempt to gain network access to facilitate persistent access
- Coalfire will leave behind malicious devices, such as thumb drives, network drives, CD's

Hoover did not receive a copy of the ROE. Shirley reviewed it but reported that nothing stood out to him besides the misidentification of testing to be done at the Warren County courthouse. Headlee stated that he did not review the ROE prior to the testing.

On August 14, 2019, there was a kick-off call with people from Coalfire and SCA. The people from Coalfire were Neumann; Dana Mortaro, Project Manager; Jakob Nelson ("Nelson"); Justin Wynn ("Wynn"); and, Gary De Mercurio ("De Mercurio"). Nelson was a penetration tester but did not participate in the physical testing in Iowa. Wynn and De Mercurio were the two penetration testers, or assessors, who later traveled to Iowa. Shirley and Hoover attended for the SCA. Headlee explained that he asked Hoover to participate in this kick-off call because Hoover asked to be involved and because of his technical knowledge of the systems to be tested. Headlee was invited to the call but declined, because he was on vacation. Headlee stated he never talked to Coalfire representatives about the 2019 testing.

This kick-off call included an online GoToMeeting interface so Coalfire presented the ROE on the screen, discussed it among the group, and edited the document in real-time. On this call, Hoover specifically requested that the phrase "[f]ocus on breaking in after-hours" be removed. It was replaced with "[c]an be during the day and evening." The only other change made to the description of the physical security assessment was that the Warren County courthouse was taken out and replaced with the Judicial Branch building.

There are competing versions of the specific discussions that occurred on the kick-off call about a physical security assessment. Coalfire's position is that after-hours testing was discussed

on the call. Neumann stated that, during the call, they talked about times of testing for the physical attacks, and “Iowa’s representative said that both before and after-hours testing was acceptable and allowed.” Neuman said he specifically asked Shirley to verify and make sure that the contacts on the ROE were going to answer their phones after hours if called. Mortaro explained that she understood that the SCA requested the change in the ROE from “[f]ocus on breaking in after-hours” to “[c]an be during the day and evening” because the SCA wanted Coalfire to make a physical assessment during the day as well. Mortaro explained that the limitation on testing activities to 6:00 a.m to 6:00 p.m. Mountain Time was only intended to cover non-physical testing. According to Nelson, Shirley specifically stated that he wanted Coalfire to put an emphasis on after-hours testing.

The SCA’s position on what happened on the call is a little different. Hoover explained that he requested the change to the ROE because he did not think it was important to test the ability to access buildings after hours; rather, he thought the real purpose of the testing was to try to access locked server closets, locked wire rooms, work stations, and other restricted areas *within* the buildings when testers were already inside. According to Shirley, participants on the kick-off call did discuss trying to penetrate the Judicial Branch building after hours but did not specifically discuss penetrating the county courthouses after hours. However, when pressed in his interview with FaegreBD, Shirley admitted that the ROE’s statement that physical testing “[c]an be during the day and evening” reflected that it could be done at county courthouses after hours.

4. Rules of Engagement

The final ROE was signed by Mortaro from Coalfire and Shirley from the SCA. It was dated, August 21, 2019. It described the “[p]hysical assessment” to be conducted by Coalfire as follows:

- Attempt to gain physical documentation at three locations
 - Polk County Courthouse
 - 500 Mulberry Street, Des Moines, IA 50309
 - More security here
 - Judicial Building
 - 1111 E. Court Ave., Des Moines, IA 50319
 - Dallas County Courthouse
 - 801 Court Street, Adel, IA 50003
- Can be during the day or evening
- Talk you [sic] way in to area, limited physical bypass
- Attempt to physical gain internal network access
- Attempt to gain network access to facilitate persistent access
- Coalfire will leave behind malicious devices, such as thumb drives, network drives, CD’s

The final ROE also stated that all penetration testing was expected to be conducted: “During normal business hours: Monday through Friday between the hours of 6AM and 6PM

Mountain time.” However, it is unclear whether this was intended to apply to the physical testing conducted in Iowa, which is Central time, especially as it was previously noted that physical testing may occur in the “evening.”

In addition, the final ROE had a section entitled, “Information Required for the Physical Security Assessment”:

INFORMATION REQUIRED FOR THE PHYSICAL SECURITY ASSESSMENT	
How many target locations are in scope for the physical security assessment?	3
In a prioritized listing, please provide the physical addresses of the facilities where physical security assessment is to be performed.	<p>JB Building 1111 E. Court Ave. Des Moines, IA 50319</p> <p>Polk County 500 Mulberry St. Des Moines, IA 50309</p> <p>Dallas County 801 Court St. Adel, IA 50003</p> <p>Juvenile Justice 222 5th Avenue 50309</p> <p>Criminal Court Area 206 6th Avenue 50309</p>
Does Coalfire have permission to tail-gate, that is, attempt to gain physical access to your facilities by following employees into the building?	Yes
Does Coalfire have permission to dumpster dive, that is, search through garbage cans and/or dumpsters on your property for sensitive information?	Yes
Does Coalfire have permission to access all areas inside the building(s)? If not, please list areas where access is not permitted.	JB Building, floors 3 & 4 no access 3 & 4 are out of scope period. May show proof of concept to access it.
If physical access is gained to your facility, does Coalfire have permission to attempt logical access to the network, including plugging into a conference room or office Ethernet jack, attempting to join the network, and then attempting further reconnaissance (ping sweep) activities?	Yes

Does Coalfire have permission to perform lock-picking activities to attempt to gain access to locked areas?	Yes
Does Coalfire have permission to strategically place hardware (USB drives, mice, keyboards, netbooks) around the building?	Yes
Does your company use proximity readers with access cards, badges or key fobs? If so, can you specify the technology? (Vendor make and model and card type?)	[Redacted by FaegreBD]
Does your network use DHCP or static IP addressing?	[Redacted by FaegreBD]
Is egress filtering employed on the network? If so, please provide allowed outbound ports. 80,443,53 etc.	[Redacted by FaegreBD]
Do you employ any physically armed personnel at the location(s) that will be tested?	Yes Polk County Courthouse (armed) State Troopers periodic sweep of Judicial building after hours 5pm - 6 am (post 16 capital)
Do you have 24/7 surveillance monitoring in place at the locations to be tested?	Yes
Are any facilities or areas of buildings or the office complex to be excluded? If so, please list here and provide reasoning for exclusion.	Polk County Criminal Court Building, armed security
Will local law enforcement or security personnel be notified that a penetration test is taking place on the specified dates?	No
What assets or areas inside the target location are of most concern in regard to physical access?	Computer Room Switch Closets

5. Authorization

The Authorization, a.k.a. the “get out of jail free” letter, identified vital information in case the assessors are confronted by security or law enforcement. It identified the assessors, the dates of testing, and the point of contacts from SCA. It listed the points of contact as Shirley, Headlee, and Hoover, and included their office and mobile numbers (though, Hoover’s mobile number was incorrect). Importantly, it also identified the tasks that could be included and the tasks that should not be performed. It stated:

Under a contract with Iowa Court Information System pursuant to Service Order #0417-19-ICIS RT, Coalfire has been requested to perform Physical Social Engineering to attempt to gain access to Iowa Court Information System resources. These attempts may include any of the following tasks:

- Impersonating staff, contractors, or other individuals
- Providing false pretenses to gain physical access to facilities
- “Tailgating” employees into facilities
- Accessing restricted areas of facilities

Tasks that shall not be performed include:

- Alarm subversion
- Force-open doors
- Accessing environments that require Personal Protective Equipment

The Authorization was signed by Shirley, Headlee, and Hoover, and dated, August 9, 2019.

6. Reporting to SCA Leadership

There was limited reporting of the details of the physical penetration that was to take place to the State Court Administrator or the Iowa Supreme Court. However, it was reported. Nuccio, the State Court Administrator, stated that he regularly met with Headlee and discussed the need for penetration testing to be performed on a regular basis. On June 18, 2019, Headlee and Shirley attended the Judicial Technology Committee meeting and the minutes of that meeting reflect a report on “Intrusion Testing”:

Red Team Testing: IT has engaged the services of Coalfire to perform a Red Team Test on our facilities. The testing will include tests with physical intrusion, social engineering and network vulnerabilities. Coalfire will not take advantage of any weaknesses, but rather point out areas of improvement. We have previously used Coalfire for a Red Team Test, which will give us a good opportunity to see areas we have improved upon since the last test.

In addition, on August 28, 2019, there was a Supreme Court retreat where cyber security penetration testing was identified as an ongoing initiative.

7. Legal Review

There was no legal review of the Coalfire documents prior to testing. Newell confirmed that she did not review the Coalfire documents and was not involved with the Coalfire testing. Shirley also confirmed that no attorney reviewed the Coalfire documents prior to testing.

D. Testing

Coalfire’s testing of the SCA’s network and facilities was scheduled to take place from August 19, 2019, to September 27, 2019. The physical testing was scheduled to take place from September 9 – 13, 2019. As the network testing began, Wynn sent Shirley and Hoover daily updates. Wynn and De Mercurio then flew out to Iowa to begin physical testing by September 9th. Shirley said he never met Wynn or De Mercurio in person. The next Shirley or Hoover said they heard from them was on September 10th. Hoover found a card from Wynn on his desk when he got into the office on that morning. Hoover congratulated Wynn via email and then informed Headlee and Shirley that the Red Team had been in the building. Hoover checked with Judicial Branch building security and learned that video surveillance footage showed Wynn and De Mercurio had been in the Judicial Branch building late the previous night of September 9th. Hoover let Headlee and Shirley know about the Red Team’s activity the previous night.

According to security, Wynn and De Mercurio appeared to have begun attempting entry into the building at 9:13 p.m., successfully entered at 9:52 p.m., and exited at 12:21 a.m. When asked by FaegreBD, Hoover and Headlee said it did not register with them that, if Wynn and De Mercurio had come into the Judicial Building after hours, they might also enter courthouses after hours. Shirley said he had expected Wynn and De Mercurio to attempt to enter the Judicial Building after hours but not the courthouses.

According to news reports, Wynn and De Mercurio entered the Polk County courthouse shortly after midnight on September 10th. This would appear to have occurred after the testing of the Judicial Branch building. However, Shirley, Headlee, and Hoover all said they were unaware that Wynn and De Mercurio went into the Polk County courthouse until hearing about it in the news.

E. Arrest of Coalfire Employees

In the early morning hours of September 11, 2019, the Dallas County Sheriff's Office arrested Wynn and De Mercurio inside the Dallas County courthouse. Shirley recalls that he was awakened by a call from Dallas County law enforcement around 1:45 a.m. on September 11th informing him that Wynn and De Mercurio had been caught breaking into the Dallas County courthouse. Shirley believed the Authorization "covered this situation" and told law enforcement. Dallas County law enforcement also called Headlee. According to Headlee, it was his position that Wynn and De Mercurio were not supposed to access courthouse after hours and so he told the Dallas County Sheriff Deputies that Wynn and De Mercurio were not working within the scope of what SCA contracted with them to do. In subsequent text messages, Headlee questioned what Wynn and De Mercurio were doing in the courthouse after hours. In text messages to Hoover, Headlee pointed out that the Dallas County Sheriff's office did not believe the Authorization applied because the courthouse was county property. Hoover replied that he was just thinking about that issue. It appears neither law enforcement, Wynn, nor De Mercurio contacted Hoover directly that night, because Hoover's number was incorrect on the Authorization form.

The Dallas County Sheriff's Office has taken the position that the SCA did not have the authority to authorize after-hours access to the Dallas County courthouse because it is owned by the county. It arrested Wynn and De Mercurio for burglary third degree, in violation of Iowa Code § 713.6A(1), and possession of burglar tools, in violation of Iowa Code § 713.7. No charges have been filed in Polk County.

Analysis

A. Confusion Over the Parameters of Red Team Testing

FaegreBD's investigation revealed disagreement and confusion over the meaning and purpose of the physical Red Team testing. FaegreBD found that misunderstandings arose around general terms that are common within cybersecurity circles but not among non-technical professionals. In addition, FaegreBD found that misunderstandings arose from the descriptions of Red Team activity within the 2019 SCA-Coalfire agreement itself.

1. Misunderstanding “Red Team” Techniques and Terminology

In this matter, FaegreBD found that non-technical professionals did not know about the full spectrum of tools and techniques that might be used by a Red Team. FaegreBD found that the highly technical professionals involved in planning the 2019 assessment understood that Red Teaming could involve aggressive techniques such as “lock-picking” a building, by-passing alarm systems, and entering a guarded building at night. This certainly was the perspective of Coalfire, which included a “[f]ocus on breaking in after-hours” in its original proposed Rules of Engagement. Shirley, the SCA’s own Information Security Officer, also understood that the Coalfire assessors could attempt to enter buildings at night, though he was focused on the Judicial Building. Even Headlee and Hoover did not immediately react when Wynn left his business card behind and they learned that the Coalfire assessors had entered the Judicial Building on the night of September 9th.

In contrast, the reaction of the SCA Administrator, the county sheriffs and other non-technical individuals was often one of shock or dismay because they did not receive a description or notice of the aggressive actions that could be associated with Red Teaming. Adding to the confusion, many Red Team techniques and terms seem at odds with common-sense. Terms like “breaking-in,” “lock-picking,” accessing “restricted areas,” and distributing “malicious devices” often refer to criminal activity in the real-world but could refer to authorized activity in a Red Team exercise. In short, FaegreBD found that the Dallas County arrests sprang in part from a language gap between technical and non-technical professionals.

2. Ambiguous Terms within the Coalfire Agreement

FaegreBD found that generally confusing Red Team concepts were compounded by ambiguities within the Coalfire agreement. First, the Coalfire agreement is not one document but rather a combination of several different documents:

- Master Agreement with Coalfire
- Service Order
- Penetration Test Rules of Engagement (“ROE”), including:
 - Scope of Testing
 - Project Logistics – Assumptions and Limitations
 - Request for Information (“RFI”)
 - Penetration Testing Methodology, and
 - Appendices (describing specific methodologies), and
- Social Engineering Authorization

Second, these different documents contained some confusing and contradictory terms. In terms of techniques, the Coalfire agreement often co-mingled descriptions of physical tests with other types of assessments. In its initial Service Order, Coalfire clearly described a plan to conduct “Physical Attacks” against three proposed buildings, but in later forms, Coalfire’s Red

Team activities fell under the more abstract label of “Social Engineering,”⁴ even though a night-time building break-in would probably not involve social interaction with any other individuals. Even Coalfire’s “get out of jail free” letter was labeled a “Social Engineering Authorization.” This Authorization allowed softer techniques like “impersonating staff” and forbade “alarm subversion” and “force[d] open doors” but did not mention prowling techniques that could be used at night.

More generally, both SCA and Coalfire appeared to co-mingle physical tests with online “pen” tests when they spoke about the 2019 assessment. One update to the Judicial Technology Committee in June 2019 did clearly explain that a Red Team Test could include “tests with physical intrusion,” but the SCA-Coalfire ROE described physical building assessments within a more general document called “Penetration Test.” Other documents, as well as many people FaegreBD interviewed tended to conflate online “pen” testing with Red Teaming. Not surprisingly, Nuncio admitted that he could not distinguish between the two. As a result, the potential for a personal confrontation with police was easily lost in the terms of the contract.

Most importantly, as described above, the SCA/Coalfire agreement contained inconsistent terms regarding the approved *timing* of a physical assessment. The Assumptions and Limitations in the ROE stated:

Project Schedule:

- All penetration testing is expected to be conducted:
 - During normal business hours: Monday through Friday between the hours of 6AM and 6PM Mountain time. NOTE: Requests for testing outside of the above approved time periods may result in additional charges per the terms of the MSA

However, the Scope of Testing in the ROE said that physical assessments “Can be during the day *and evening*.” (p. 4, emphasis added). The Authorization did not mention time of day at all.

3. Inconsistency Between the 2015 and 2019 Red Team Assessments

Separately, some key SCA employees understood that the 2019 assessment would follow the pattern of Coalfire’s 2015 engagement. In particular, both Headlee and Hoover stated that they saw little need to try to break into county courthouse because that was not the main point of the Red Team exercise. Headlee had signed the 2015 contract and had thoroughly reviewed the results of the 2015 “Red Team Test Summary Report” from Coalfire. In that test, Coalfire assessors talked their way past security personnel, gained access to empty rooms or restricted areas, and left behind thumb drives or digital “drone” devices, but assessors had restricted their activity to work-day hours and had not broken into any buildings. Headlee assumed that the 2019 assessment would proceed in manner similar to the 2015 assessment.

⁴ Coalfire is not alone in describing its Red Team tests as “social engineering.” Other cybersecurity firms also described physical building tests under the heading “social engineering” in their proposals submitted in the spring of 2019.

B. Lack of Oversight

FaegreBD found that many of the missteps leading to the Dallas County arrests could have been avoided with better oversight of the contracting process with Coalfire and the assessment itself. Nuncio stated that he felt that the Judicial Branch IT (JBIT) contracting process needed stronger oversight in general, and we agree. The Coalfire contract was largely formed by Shirley, with some input from Hoover. Headlee signed off on the contract but did not know the details about specific conversations with Coalfire, and no attorney had reviewed the contract in general. A legal review of the contract, or even a review by a senior non-technical leader like Nuncio likely would have generated practical concerns and questions. This type of assessment should have included input from physical security professionals as well. We believe this would have led to more precise contract terms, clearer and less aggressive testing of judicial buildings, and more timely notice to county officials.

Coalfire went almost silent during the building tests themselves. In fact, many SCA managers did not know that Wynn and De Mercurio had entered the Polk County courthouse until days later when the news broke. We believe that more aggressive daily oversight by the SCA and more regular check-ins by Coalfire during the physical Red Team testing would have produced better results and fewer surprises.

C. Failure to Appreciate the Impact on Third Parties

Perhaps the greatest shortcoming we found was a failure to take into account the potential impact of the assessment on third parties, specifically the counties. We did not find that the SCA or Coalfire acted with deception or ill-intent. However, we believe both the SCA and Coalfire should have foreseen a potential confrontation with law enforcement. The Coalfire RFI asked pointed questions about armed personnel, 24/7 surveillance, shared space within building facilities, permission to access all building areas, and potential notice to law enforcement or security personnel. Perhaps most telling, both the SCA and Coalfire knew that assessors would carry a document they had jointly labeled, a “get out of jail free” memo. Therefore, a run-in with law enforcement seemed likely, or at least possible.

This Red Team test should have included special precautions, given that the SCA is a government agency with many public partners. The SCA/Coalfire agreement did limit assessments on floors 3 and 4 where the Court of Appeals and Supreme Court sit within the Judicial Building. The SCA also warned Coalfire assessors to avoid the Polk County Criminal Court Building with its armed security. However, the SCA did not offer similar warnings about the Dallas County courthouse and nobody notified the sheriffs in either Polk or Dallas Counties. Finally, neither the SCA or Coalfire took into account that the Red Team would be test the security of a public building on 9/11, a national day of mourning and general unease.

Perhaps the SCA did not think of notifying county officials because they thought the tests would follow the innocuous pattern of 2015. If so, they still missed an opportunity to correct course on September 10th when Hoover received Wynn’s “calling card” and learned that Wynn and De Mercurio had entered the Judicial Building the previous night. Shirley thought the entry was expected and authorized, while Headlee and Hoover admitted they were more focused on

the techniques Wynn and De Mercurio had used to get in, not the timing of their actions. Upon receiving Wynn’s card, Hoover replied: “Well done. I’ll be interested to hear how easy it was.” In short, the technical experts overlooked the risks of a physical assessment. This is where greater oversight and control by a non-technical administrator and input from physical security professionals could have been helpful, potentially raising the alarm about additional night-time prowling.

D. The SCA’s Authority to Grant Coalfire Access to County Courthouses

Lastly, it is unclear whether the SCA had the legal authority to grant Coalfire access to the county courthouses after hours. Iowa’s counties are required by statute to “provide the district court for the county with physical facilities,” including necessary amenities such as “heat, water, electricity, maintenance, and custodial services.” Iowa Code § 602.1303(1). The facilities provided by the county must include “courtrooms, offices, and other physical facilities” that are “suitable for the district court, and for judicial officers of the district court, the clerk of the district court, juvenile court officers, and other court employees.” *Id.* § 602.1303(1)(a). The facilities must also include “suitable offices and other physical facilities for the district court administrator and staff” as deemed necessary by the chief judge of the judicial district. *Id.* § 602.1303(1)(b). According to the Iowa Attorney General, “[o]n the failure of the county to provide sufficient facilities, the court itself, to insure the efficient administration of justice, has not only the right, but also the duty, to see that it is properly equipped in its accommodations and furnishings so as to be able to act effectively as a court.” 1990 Iowa Op. Atty. Gen. 66, 1990 WL 484887 at *2 (Iowa A.G. March 7, 1990) (quoting *Castle v. State*, 143 N.E.2d 570 (Ind. 1957)).

Though the term “sufficient facilities” as used in these authorities would ultimately need to be subject to judicial interpretation, it is a colorable reading of the statute and the Attorney General’s opinion that the facilities provided by the county must be physically and electronically secure to be considered “sufficient.” Under such a reading, the Judicial Branch has both a right and a duty to ensure all district court facilities are secure. *Accord* Opinion No. 03-4-1, 2003 WL 22100958, at *3 n.2 (Iowa A.G. April 7, 2003) (“[T]he judiciary has inherent power to adopt any measure to ensure the ‘immediate, necessary, efficient, and basic functioning of the courts.’” (quoting *Webster Cty. Bd. of Sup’rs v. Flattery*, 268 N.W.2d 869, 873 (Iowa 1978))). Indeed, the Attorney General has previously opined that the counties actually lack authority over the facilities they are required to provide for the district courts’ use—*i.e.*, the security of the facilities may in fact be in the *exclusive* province of the Judicial Branch. *See* Opinion No. 88-1-11(L), 1988 WL 1583201, at *1 (Iowa A.G. Jan. 21, 1988) (“While the counties are required to provide suitable facilities for the Courts, . . . nothing in the statutes reserves authority over the use of those facilities for the counties.”).

Notably, none of the statutes, cases, or advisory opinions on this topic discuss how the courts’ autonomy is affected when the county-provided court facilities share their premises with other non-court facilities. It appears to be an unresolved question whether the courts’ authority extends inherently to the entire building in which its facilities are housed or only the portions set aside for judicial and court administrative functions. In 2017, the Supreme Court touched upon this ambiguity when it issued two Supervisory Orders establishing a “statewide policy

prohibiting all weapons from courtrooms, court-controlled spaces, and public areas of courthouses and other justice centers.” *In re Courthouse Security, Supervisory Order I* (Iowa June 19, 2017). In the second of the two orders, the Court stated its understanding that “courthouse security in Iowa is an ongoing and shared responsibility with county boards of supervisors, county officials, and others.” *In re Courtroom Security, Supervisory Order II* (Iowa December 19, 2017). To that end, it permitted county boards of supervisors to request in writing that public non-court-related areas of county courthouses be excluded from the statewide firearms prohibition. *Id.* The Court defined a “courthouse” over which it would assert authority, as “any building in which the court system occupies space.” *Id.* In so doing, the Court *presumed* that it held authority over all areas (including non-court-controlled areas) and that it could partially relinquish that authority. The Court’s presumption that it holds inherent (and relinquishable) authority over those physical spaces does not appear to have yet been tested in litigation.

In the broadest possible terms, judicial autonomy is established in the foundations of the Iowa Constitution, which grants the Supreme Court the power to “exercise a supervisory control over all inferior judicial tribunals throughout the State.” Iowa Const. Art. V, § 4. But the following two questions about the limits of that autonomy have not been fully and finally determined: (1) whether the Court’s power extends without limitation to testing and improving security through any possible means; and, (2) whether the Court’s power extends without limitation to non-court-related areas of a building that includes court facilities. Based upon the language of the statutes, orders, cases, and opinions cited above, it is likely that the Supreme Court *does* have full authority to manage security of its assigned facilities and systems—including testing—without limitation. The Court has also asserted authority over non-court-related areas of the county courthouses throughout the State. Assuming both of these conclusions are accurate, the Court *did* hold sufficient authority to grant Coalfire permission to enter the premises. However, both assumptions may be subject to colorable legal challenges, and if either conclusion is not ultimately borne out, the Court likely did *not* have authority to grant Coalfire permission to enter the shared public (non-court) areas of the county courthouses.

Conclusions & Recommendations

Based on these findings of fact and analysis, FaegreBD makes the following conclusions and recommendations:


A. Conclusions

1. **Misunderstanding of Red Team Testing.** The SCA’s lack of experience with and understanding of Red Team testing contributed to the misunderstanding between the SCA and Coalfire as to whether Coalfire was supposed to conduct physical testing of county courthouse facilities after hours.
2. **Ambiguous Language in Coalfire Agreement.** The language in the SCA’s agreement with Coalfire was ambiguous and also contributed to the misunderstanding between the SCA and Coalfire.

3. Lack of Management & Oversight. In addition, there was a lack of management and oversight that contributed to the misunderstanding between the SCA and Coalfire. Specifically, we find:
- a. **Failure to Identify Issue:** Shirley was tasked to lead the penetration testing. He did not seem to understand that the SCA may not have legal authority to authorize access to county courthouses after hours or the potential sensitivity around conducting physical testing at county courthouses after hours. Accordingly, he did not raise that as an issue with superiors or Coalfire. Hoover worked with Shirley on the testing. He seems to have missed the issue as well, and therefore also did not raise it. However, he was not the lead on the task and his involvement seems to have been more of a technical role.
 - b. **Failure to Supervise Testing:** Headlee appears to have understood that there might be an issue with the SCA granting Coalfire access to county courthouses after-hours. However, Headlee did not raise that issue with Shirley. Likewise, Nuccio seems to have understood that granting Coalfire access to county courthouses after hours might be an issue, but he did not discuss it with Headlee.
 - c. **Failure to Review Agreement:** SCA had its own legal counsel, but there was a lack of any legal review by the SCA of the agreement between the SCA and Coalfire.
4. Unclear Authority Over Courthouse Security. Lastly, it is unclear whether the SCA had the legal authority to grant Coalfire access to the Polk County and Dallas County courthouses after hours.

B. Recommendations

1. Provide Stronger Oversight of IT Security Contracts. We recommend that IT contracts receive a legal review, particularly those that involve sensitive security testing methods. In addition, we recommend that the State Court Administrator sign off on any penetration” or Red Team testing in the future. Red Team planning also should include input from building security, sheriffs, or other physical security professionals.
2. Add More Precision in the Agreement. We recommend that Penetration or Red Team contracts contain fewer documents and more precise terms. In particular, we recommend that permitted and prohibited techniques be defined more explicitly. We also recommend that “Physical Testing” be addressed as its own category, separate from “Penetration Tests” or “Social Engineering.”

- 
3. Prohibit Entry of Buildings Outside of Normal Work Hours. We recommend that the SCA apply the same time restrictions used in Coalfire’s 2015 assessment. This assessment appeared to produce helpful results without controversy. The nighttime or “after-hours” testing was the main problem in this matter.
 4. Confer with Other Officials before Running Security Assessments. Most importantly, we recommend that the SCA confer with sheriffs, other local officials, or other state supervisors that could be affected by a security assessment, especially of a mixed-use or jointly administered building. Often the physical testing of a site is secondary to the network assessment, so little will be lost by providing notice. Moreover, safety should override any desire to conduct a stealthy assessment.