

Summer 2025 Access Control Drill AAR-IP

To view the formatted PDF, click here: [Summer 2025 Access Control Drill AAR-IP.pdf](#)

Summer 2025 Access Control Drill

After-Action Report/Improvement Plan

August 22, 2025

Non-Confidential (NC): This document does not contain sensitive and/or confidential information. It is available for public inspection.

Exercise Overview

Exercise Name	Access Control Drill
Exercise Date	June 24-26, 2025
Planning Date	None
Hotwash Date	August 6, 2025
Scope	This exercise is a drill and evaluates the ability of appropriate agencies to be able to effectively control access to campus buildings and spaces. The scope was limited to testing whether the intended result from the access restriction was successful at each applicable door. Participants utilized radio communications for reporting based on an Incident Radio Communications Plan (ICS 205).
Focus Areas ^[1]	Prevention, Protection, Mitigation, Response
Core Capabilities ^[2]	§ Access Control and Identity Verification § Infrastructure Systems § Interdiction and Disruption § Planning
Target Capabilities	§ Quickly restrict access to campus buildings and spaces § Quickly restore access to campus buildings and spaces § Ensure proper management, maintenance, and training of access control systems

Exercise Name	Access Control Drill
After Action Report	
Organization	Arkansas State University
Lead Agency	Office of Emergency Management
Participating Organizations	Blue Sky Technologies, Facilities Management, Information and Technology Services, University Housing, University Police Department Note: Multiple campus offices/departments assisted in the drill phase.
Point of Contact	Wyatt Reed , Emergency Operations and Occupational Safety Specialist Office of Emergency Management Arkansas State University WReed@AState.edu or (870) 972-3352

Analysis of Capabilities

Table 1 includes the exercise objectives, aligned capabilities, and performance ratings for each capability as observed during the exercise and determined by the evaluation team.

Target Capabilities	Core Capability [3]	Performed without Challenges (P)	Performed with Some Challenges (S)	Performed with Major Challenges (M)	Unable to be Performed (U)
Quickly restrict access to campus buildings and spaces.	Access Control and Identity Verification	X			
	Interdiction and Disruption		X		
	Planning	X			
Quickly restore access to campus buildings and spaces.	Access Control and Identity Verification	X			
	Planning	X			
Ensure proper management, maintenance, and training of access control systems.	Access Control and Identity Verification		X		
	Infrastructure Systems		X		
	Interdiction and Disruption		X		

Target Capabilities	Core Capability [3]	Performed without Challenges (P)	Performed with Some Challenges (S)	Performed with Major Challenges (M)	Unable to be Performed (U)
Planning		X			

Table 1. Summary of Core Capability Performance

Rating Definitions:

Performed without Challenges (P): The targets and critical tasks associated with the capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. The performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Performed with Some Challenges (S): The targets and critical tasks associated with the capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. The performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.

Performed with Major Challenges (M): The targets and critical tasks associated with the capability were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Unable to be Performed (U): The targets and critical tasks associated with the capability were not performed in a manner that achieved the objective(s).

The following sections provide an overview of the performance related to each exercise objective and associated capability, highlighting strengths and areas for improvement.

Capability Definitions:

Access Control and Identity Verification: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

Infrastructure Systems: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

Interdiction and Disruption: Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.

Planning: Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Exercise Design

Initial Design

The initial design of this exercise was executed by the A-State Campus Card Center, a division of Information Technology and Services. The goal of the exercise was to evaluate the performance of access control systems by evaluating the capabilities of the utilized software and evaluation of the physical hardware to respond to the software's command.

Campus administration and safety personnel were notified of the testing plan roughly 8-10 days before the planned execution of the exercise. While this was a rapid turnaround, previous campus safety threats underscored the need to ensure the test was performed ahead of the Fall 2025 semester to evaluate the access control systems' current efficacy and to mitigate any problems with the systems ahead of students' arrival in August. However, this also offered little ability to significantly alter the design plan and to fully understand the design.

The initial design called for 15-minute testing periods within a 4-hour window. One building would be tested within that 15-minute testing period, except when the size of the building would justify including more buildings within the same testing period.

Resources needed included:

- **Contractors:** Contractors from Blue Sky Technologies were on-site to assist with hardware and software-related issues.
- **Personnel:** Personnel physically evaluated and verified the status of access control doors, as well as activating/deactivating software and responding to hardware issues.
- **Radios:** The Chief of University Police procured radios to disperse to personnel assisting with the exercise. Additional portable radios were brought by certain participating departments that already had them.
- **Software:** A software program was utilized to develop shortcuts (also known as "threat levels") to quickly effect the desired outcome.
- **Temporary Card Access:** Temporary cards had to be printed with basic all-access and with UPD-only all-access for personnel to assess the access control systems.
- **Transportation:** While the exercise group often sought to test buildings near each other, ultimately, university and private vehicles, golf carts, etc., were utilized to move personnel from one test site to another.

Design Adjustments

The main initial design was adjusted to be performed in 3 days, not 2. Additionally, testing windows were moved from 15-minute periods to 20-minute periods (generally). As the drills were performed, the schedule was altered based on available personnel and needs.

Issues Identified:

- Planning was not adequately performed for this exercise. A longer planning period was needed, and more stakeholders needed to be involved in that plan.
 - Drill evaluation forms contained unclear or misleading questions that produced a likely bias and/or holes in the data.
 - Personnel were not pre-identified or assigned. This caused scheduling issues. For example, when available personnel did not meet the demand for the number of doors being tested, time delays were created. When available personnel exceeded scheduled needs, the schedule was changed without advance notice, causing operational impacts to campus members.
 - Respondents to the participant survey noted a lack of available transportation.
 - There were too few resources, such as radios and access cards.
- More periodic preventative maintenance checks on access-controlled doors are needed.
 - While it would be unreasonable to expect the physical infrastructure of all access-controlled doors on campus to always function properly, more resources and planning seem needed to identify hardware issues as they occur on access-controlled doors.
- Accessibility issues continue to plague campus access.
 - ADA issues were prevalent – many ADA-type features were unable to be tested on access-controlled doors because ADA devices were not installed.

Successes Identified:

- The planning within the software worked exactly as planned, and few (if any) software failures were noted throughout the drills.
- The access-controlled capability worked exceptionally well, and the process to control spaces has been and is continuing to be drastically improved upon. UPD's Dispatch Center will soon be able to activate and control these systems even quickly.
- Campus involvement in the drill was outstanding, especially given the particularly busy time of the year, short notice, and last-second scheduling changes.

Data Categorization Process

The supporting sample data that informed the results presented in the next section was collected through evaluation forms that participants completed for each door and scenario. The data is classified as follows:

- Working Appropriately: all features of the door worked as expected in permitting or restricting access in accordance with the expected result. A door that is working appropriately needs no further action at this time.
- Partial Failures: a feature(s) of the door did not work as expected; however, the ability to control access remained intact, or at least maintained a fail-secure state.

- ADA-Only Failures: the accessibility features of the door were the **only** feature of the infrastructure that did not meet the access control expectations.
- Complete Failures: a feature(s) of the door did not work as expected and, as a result, the ability to control access was lost.
- Unable to Test: an issue or fact existed that prevented the ability to effectively and/or fairly test the ability to control access.

NOTE: each door was only counted in one of these categories. For instances where more than one condition could apply, the most applicable category is applied.

Common Issues

Many of the same types of issues were noted within each respective category. 89 access-controlled spaces were logged as having issues. Of these 89, 52 (58.43%) required a work order to be fixed. The remaining doors were either fixed on site or another fact existed that did not require the submission of a work order. Of the 52 submitted, 27 (51.92%) have been closed while the rest remain open. Common issues included:

- Physical failures (broken locks, broken doors, missing infrastructure, etc.)
 - Most issues noted were due to some physical failure. These could be greatly reduced through more routine maintenance and proper usage by the campus community.
- Technology failures (communication failures, glitches, etc.)
 - These primarily existed when the hardware did not respond to the technology's commands. The software, by and large, worked appropriately.
- ADA failures (missing infrastructure, etc.)
 - Data probably has a gap here, as the exercise was not intended to robustly test our ADA system's integration and infrastructure.

Normal Access Mode

In the Normal Access Mode, access is granted based on the normal permissions of the door. Both the base all-access card and the UPD-only all-access card should grant entry.

Unadjusted Results:

- Working Appropriately:
 - Regular Card: 280 of 317 (88.33%)
 - UPD-Only Card: 282 of 317 (88.96%)
- Partial Failures:
 - Regular Card: 8 of 317 (2.52%)
 - UPD-Only Card: 3 of 317 (0.95%)
- Complete Failures:
 - Regular Card: 6 of 317 (1.89%)
 - UPD-Only Card: 1 of 317 (0.32%)
- Unable to be Tested:
 - Regular Card: 23 of 317 (7.26%)
 - UPD-Only Card: 31 of 317 (9.78%)

Discrepancies: Normal Access Mode results are based on the data from the Inclement Weather Access Mode test. As a result, there is no means in place to verify the correct starting state of the doors. It is assumed that the starting state of the doors was correct relative to those doors scheduled state. If a door was locked or unlocked when it was scheduled to be the opposite, that will not be reflected as a failure in the results.

Inclement Weather Access Mode

In the Inclement Weather Access Mode, access is granted based on the normal permissions of the door. Both the base all-access card and the UPD-only all-access card should grant entry. No other changes, EXCEPT: in the Student Union, all exterior doors with access control should unlock with no card required for entry.

Unadjusted Results:

- Working Appropriately:
 - Regular Card: 300 of 344 (87.21%)
 - UPD-Only Card: 299 of 344 (86.92%)
- Partial Failures:
 - Regular Card: 8 of 344 (2.33%)
 - UPD-Only Card: 3 of 344 (0.87%)
- Complete Failures:
 - Regular Card: 11 of 344 (3.20%)
 - UPD-Only Card: 6 of 344 (1.74%)
- Unable to be Tested:
 - Regular Card: 25 of 344 (7.27%)
 - UPD-Only Card: 36 of 344 (10.47%)

Discrepancies: There is no means in place to verify the correct starting state of doors. It is assumed that the starting state of the doors was correct relative to those doors scheduled state. If a door was locked or unlocked when it was scheduled to be the opposite, that will not be reflected as a failure in the results.

UPD-Only Access Mode

In the UPD-Only Access Mode, access is no longer granted based on the normal permissions of the door. The base all-access card should not grant entry. The UPD-Only all-access card should grant entry.

Unadjusted Results:

- Working Appropriately:
 - Regular Card: 259 of 344 (75.29%)

- UPD-Only Card: 215 of 344 (62.50%)
- Partial Failures:
 - Regular Card: 5 of 344 (1.45%)
 - UPD-Only Card: 8 of 344 (2.33%)
- Partial Failures (ADA Only):
 - Regular Card: 29 of 344 (8.43%)
 - UPD-Only Card: 58 of 344 (16.86%)
- Complete Failures:
 - Regular Card: 18 of 344 (5.23%)
 - UPD-Only Card: 21 of 344 (6.10%)
- Unable to be Tested:
 - Regular Card: 33 of 344 (9.59%)
 - UPD-Only Card: 42 of 344 (12.21%)

Discrepancies: 38 doors (Regular Card) and 0 doors (UPD-Only Card) were likely improperly biased during testing to be placed in the complete failures category when these doors most likely worked without issue. As a result, these doors were moved during data analysis to the working appropriately category. However, it is possible that a few of these doors should be in the complete failures category.

No Access Mode

In the No Access Mode, access is no longer granted based on the normal permissions of the door. The base all-access card and the UPD-Only all-access card should not grant entry.

Unadjusted Results:

- Working Appropriately:
 - Regular Card: 259 of 344 (75.29%)
 - UPD-Only Card: 255 of 344 (74.13%)
- Partial Failures:
 - Regular Card: 3 of 344 (0.87%)
 - UPD-Only Card: 4 of 344 (1.16%)
- Partial Failures (ADA Only):
 - Regular Card: 19 of 344 (5.52%)
 - UPD-Only Card: 16 of 344 (4.65%)
- Complete Failures:
 - Regular Card: 16 of 344 (4.65%)
 - UPD-Only Card: 15 of 344 (4.36%)
- Unable to be Tested:
 - Regular Card: 47 of 344 (13.66%)
 - UPD-Only Card: 54 of 344 (15.70%)

Discrepancies: 38 doors (Regular Card) and 37 doors (UPD-Only Card) were likely improperly biased during testing to be placed in the complete failures category when these doors most likely worked without issue. As a result, these doors were moved during data analysis to the working appropriately category. However, it is possible that a few of these doors should be in the complete failures category.

Aggregated Results

The following are the aggregated results of all specific access modes combined.

Unadjusted Results:

- Working Appropriately:
 - Regular Card: 1,098 of 1,349 (81.39%)
 - UPD-Only Card: 1,051 of 1,349 (77.91%)
- Partial Failures:
 - Regular Card: 24 of 1,349 (1.78%)
 - UPD-Only Card: 18 of 1,349 (1.33%)
- Partial Failures (ADA Only):
 - Regular Card: 48 of 688 (6.98%)
 - UPD-Only Card: 74 of 688 (10.76%)
- Complete Failures:
 - Regular Card: 51 of 1,349 (3.78%)
 - UPD-Only Card: 43 of 1,349 (3.19%)
- Unable to be Tested:
 - Regular Card: 128 of 1,349 (9.49%)
 - UPD-Only Card: 163 of 1,349 (12.08%)

Exercise Executive Notes

Overall Evaluation

Overall, the exercise was a success. This is especially true given all the specific parameters and circumstances surrounding it. More follow-up testing will be needed to verify the data collected, although it is likely a fair statistical overview.

Player Feedback

Overall Evaluation

Players overall provided positive feedback. 19 respondents completed the evaluation form out of 60 players who received the evaluation form link (a 31.67% response rate).

Player Evaluation Form

The Office of Emergency Management conducted evaluation polling via a Microsoft Form that was sent to each registered player. Respondents were given 7 days to respond to the evaluation, and responses were not compelled. The form is composed of two parts: a questionnaire utilizing the Likert Scale that was designed to collect more quantitative data, and a short answer/listing section designed to collect more qualitative data.

The success of the exercise based on the Part A evaluation results was determined using a combination of median and mode statistical analysis products (Success = $\bar{x} > 3$ AND $Mo > 3$). The success formula was based on the idea that, on average (i.e., the mean), more people should feel better than neutral about the organization and results of the exercise. In addition to that, the category with the most responses (i.e., the mode) should be in an affirmative stance ("agree" or "strongly agree") that corresponds to a positive outlook on the exercise design, results, and function.

Part A: Likert Scale Questionnaire

In all questions, the respondent was asked to rank their agreement with a statement regarding the exercise. The options were: Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), and Strongly Agree (5). All questions were worded in a positive, affirmative stance.

Question #1: The exercise seemed well planned.

Results:

- Mean: 4.21
- Mode: 4

Question #2: The exercise seemed to be punctual and stayed on schedule.

Results:

- Mean: 3.42
- Mode: {5,4,3}

Question #3: Instructions by facilitators to you were clear and effective.

Results:

- Mean: 4.26
- Mode: 5

Question #4: You felt comfortable participating in the exercise.

Results:

- Mean: 4.68

- Mode: 5

Question #5: You felt comfortable providing your input to the exercise group.

Results:

- Mean: 4.68
- Mode: 5

Question #6: You felt able to quickly identify the next steps that should be taken while assisting in the exercise.

Results:

- Mean: 4.42
- Mode: 5

Question #7: The systems used (radio, forms, etc.) aided and were useful.

Results:

- Mean: 4.42
- Mode: 5

Question #8: The physical requirements (e.g., walking, stairs, etc.) were communicated and did not pose a challenge.

Results:

- Mean: 4.47
- Mode: 5

Response Distribution Overview

Aggregated Results:

- Mean: 4.32 ($\bar{x} > 3$, SUCCESS)
- Mode: 5 ($M_o > 3$, SUCCESS)

Part B: Feedback Form

Question #1: Please list up to 3 areas of strength (things that you felt went well) noted from this exercise.

Responses included:

- Fluidity of the exercise.
- Patience, attentiveness, and flexibility of players.

- System configuration was accurate and worked as expected.
- Maintenance needs were identified, with many fixed in real-time.
- Assistance available.

Question #2: Please list 3 areas of improvement (things that you feel we could do better) noted from this exercise.

Responses included:

- More resources, including transportation and radios.
- Clearer instructions and resources, such as forms and maps.
- More comprehensive planning cycle.
- Increase campus accessibility.

Question #3: What steps would you take to rectify concerns noted in question #2?

Responses included:

- Procure more resources, including radios, transportation, and access cards.
- Send a reminder email/communication.
- Utilize the Office of Emergency Management expertise and resources in planning.
- Adding in scheduled time and processes for “onboarding” volunteers.

Final Step: Please list any additional comments or concerns that you may have.

Responses included:

- Appreciation for willingness to implement and test this system.
- Everyone’s work, effort, and patience in participating in this exercise.

Areas of Strength

Strength 1 (Access-Control Capabilities)

One of the leading strengths that was noted from our exercise is our ability to access control so many doors across campus, especially in critical spaces. While a large amount of work remains, A-State is continuously making positive strides towards a safe and secure environment by investing money, time, and personnel into access-control infrastructure. After most active threat events at universities (including larger institutions, such as Michigan State and Florida State), access control is a major point of discussion. Our software and, to a great extent, our infrastructure, worked well during this exercise. **(Capability: Access Control and Identity Verification, Infrastructure Systems, Interdiction and Disruption)**

Strength 2 (Access-Control Training and Program Management)

The Access Team that works underneath A-State ITS has seemingly done a fantastic job of building our access-control systems into a comprehensive program. In addition to expanding capacity and capabilities, this team has also worked hard to create/update access policies as well as remediate pre-existing program issues. The ITS team is continuing to expand the program and include more campus partners and training. **(Capability: Access Control and Identity Verification, Infrastructure Systems, Interdiction and Disruption, Planning)**

Strength 3 (Campus Involvement)

Another strength noted from this exercise was the willingness of the A-State campus community to unite to meet the needs this exercise required for an effective test. Numerous personnel, including students, staff, and faculty, participated in the exercise directly. Virtually the entire campus was affected at some point by restricted access, yet the campus overwhelmingly welcomed the exercise. This commitment to campus safety and security is critical to building a resilient community. **(Capability: Planning)**

Areas for Improvement

Improvement Area 1 (Planning)

The greatest area of improvement for this exercise is in planning. Better and more reliable data could likely have been collected through differently worded questions, forms, and processes. Delays and other challenges could likely have been planned for and either mitigated or prepared for with advanced planning. Additionally, better exercise design and documentation could have been available with earlier involvement of the Office of Emergency Management. **(Capability: Planning)**

Improvement Area 2 (Maintenance)

More systematic preventative maintenance checks are needed for access-control infrastructure. It has to be understood that we will never be able to always prevent one of these systems from breaking. However, the exercise revealed that we could do a better job in planning preventative maintenance and preventing the quantity/downtime of impacted infrastructure. **(Capability: Infrastructure Systems, Planning)**

Improvement Area 3 (Accessibility)

Accessibility is a concern in multiple parts of our campus operations. In this context, we likely need to better understand our expectations of ADA systems and infrastructure if a particular access mode is needed, and then plan for a way to make the ADA systems compatible and responsive to that expectation. Many infrastructure and programming failures were noted in this drill in relation to ADA systems. Most of these failures would not compromise access-controlled spaces, but the systems are still not operating appropriately. **(Capability: Infrastructure Systems, Planning)**

Appendix A.1: Exercise Day 1 Schedule

Appendix A.2: Exercise Day 2 & 3 Schedule

Appendix B.1: Exercise Day 1 ICS 205 Form

Appendix B.2: Exercise Day 2 ICS 205 Form

Appendix B.3: Exercise Day 3 ICS 205 Form

Appendix C: Improvement Plan

This IP is developed specifically for Arkansas State University as a result of the Access Control Drill conducted in June of 2025:

Area for Improvement	Corrective Item	Implementation Plan	Primary Responsible Organization	Organization POC
Planning	Exercise Design Planning	For future exercises, a more robust exercise design plan needs to be created in conjunction with the Office of Emergency Management (OEM) and other key partners.	ITS (Primary) Emergency Management (Secondary)	ITS: Heather Boothman or Bethany Adams Emergency Management: Wyatt Reed

Area for Improvement	Corrective Item	Implementation Plan	Primary Responsible Organization	Organization POC
Maintenance	Preventative Maintenance Checks	Increase preventative maintenance checks and documentation to ensure the university is limiting the number of doors that are in a “down” status, as well as the amount of time doors are in a “down” status.	ITS (Primary) Facilities Management (Secondary)	ITS: Tony Marshall or Dane Buck Facilities Management: Zone Maintenance
Accessibility	ADA & Access Control Expectations	Create a list of expectations for each related ADA system in normal and all other access mode states. Additionally, compare the results of this/future exercises to this list of expectations to determine the efficacy of ADA systems relative to access controls.	ITS (Primary)	ITS: Heather Boothman or Bethany Adams
	Increasing ADA Access	Continuing to inventory ADA capabilities and target needs to identify gaps. Create plans and solutions to allocate resources to ADA compliance initiatives.	Facilities Management (Primary) ITS (Secondary)	Facilities Management: Brian Lasey ITS: Tony Marshall or Dane Buck

[\[1\]](#) Selected from National Preparedness Goal’s Five Mission Areas (DHS, 2015)

[\[2\]](#) Selected from National Preparedness Goal List of Core Capabilities (DHS, 2015)

[\[3\]](#) Selected from National Preparedness Goal List of Core Capabilities (DHS, 2015)

Revision #3

Created 2025-10-24 19:47:56 UTC by Wyatt Reed

Updated 2025-12-01 14:46:01 UTC by Wyatt Reed