Public Venue Credentialing Guide

Commercial Facilities Sector

May 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Table of Contents

1 Executive Summary

Across the United States, **people expect that they will be safe and secure** as they cheer on a favorite team at a sporting event, attend a concert, dine out with family and friends, or engage in other activities in public places.

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) works closely with public and private sector partners to mitigate risk and protect our infrastructure. This mission includes working to secure public venues in partnership with the private sector owners and operators of these facilities, who are represented by the Commercial Facilities Sector Coordinating Council.

This Public Venue Credentialing Guide—the result of an effort to update public-private sector security recommendations to meet evolving threats—provides suggestions, guidance, and best practices for developing and implementing credentialing procedures at public venues that host large-scale events. This document expands upon the Sports Venue Credentialing Guide published in 2012 and incorporates changes and updates to credentialing policies across the Commercial Facilities Sector. To address the sector's diversity in developing the guide, the Public Venue Credentialing Guide Working Group was formed with Government Coordinating Council and Sector Coordinating Council members, including representatives from the Sports Leagues, Public Assembly, and Outdoors Events Subsectors who provided expert input based on industry priorities, concerns, and best practices.

The credentialing procedures in this guide are options for consideration and are neither definitive nor required by any regulation or legislation. Due to the wide variety of types, sizes, and locations of public assembly venues and the events held in these venues, not all suggested procedures will be relevant or applicable. Venue owners, operators, and event organizers may choose to implement any or all the options in this guide and should supplement them with additional resources, when available.

Additional guidance related to the security of the Commercial Facilities Sector, as well as other helpful information, is available at www.cisa.gov/cisa/commercial-facilities-resources.

2 Credentialing

Credentialing serves as an **access control process for individuals who desire access to or wish to move within a venue**. Credentialing programs are established to control and restrict access to and within a venue and provide venue management and staff with information on those who have access.

Credentialing can also be used to control and restrict vehicle movement within and around a venue.

2.1 What is a credential?

A credential grants an individual access to areas in a venue that require authorization. Credentials are different from tickets, which provide access via a public entrance during an event. This guide focuses on credentials and not ticketed venues or events**.** For further guidance on ticketing, please review the Patron Screening Best Practices Guide.

A strong credential is visually easy to discern and simple to use, yet difficult to falsify.

If possible, provide a hologram or other protective measure on the credential to reduce the potential for counterfeiting. This could include a radio-frequency identification (RFID), watermark, foil, or other embedded image.

Simplify the credentialing process by indicating areas of access by shapes, numbers, letters, or symbols and color-coding by event function.

- **Design and color-code the credentials** to ensure they are substantially different from those used at previous events or in prior seasons or years.
- **Sequentially number credentials** and maintain a record of each person issued a credential for control purposes.
- Ensure the credential is marked with the **time frame during which the credential is valid.**

If possible, create a credential that is "user-specific" to ensure that it is nontransferable, such as by including a photo of the user on the credential.

A credential can also serve as a resource for the user. For example, the back of a credential could describe the user's rights, the credential's restrictions, and/or the phone numbers for a venue's security or emergency response.

2.2 What are the aspects of a secure credentialing program?

A secure credentialing program should include policies and processes that ensure credentials are being used by the appropriate individuals and limit the ability to counterfeit or abuse credentials.

If possible, consider digitally signing the information on the credential. This will allow for any discrepancies between the printed and scanned information to be easily identified.

Policies should be established that prohibit the sharing of images of credentials on social media. If possible, coordinate with social media teams to monitor for possible violations of these policies, and instruct accounts to remove their posts from social media or risk the revocation of their credentials.

BEST PRACTICE

Ensure that credential users are aware that credentials can be revoked at any time if the associated terms and conditions are violated.

Credentialing systems can be made more secure by utilizing electronic systems that can activate or deactivate a credential if it is lost or stolen. Scannable credentials also provide a system to control access time and area. A secure credentialing program should include procedures for reporting and deactivating lost, expired, or revoked credentials.

Recommendations for credentialing processes are noted in Section 3.

2.3 What types of credentials exist?

Full-time and part-time venue employees should have individual credentials that clearly identify each user as a venue employee. These credentials should include **photos, swipe or proximity card access capabilities, or bar code technology**, when applicable.

Full-time contractor support personnel may either use the same credentials as full-time venue employees (this designation should be indicated somewhere on the credential) or have their own separate credentials.

A venue should issue **temporary contractors'** credentials that are work order-specific, indicate a time frame for work to be performed, and designate the area(s) of access and nature of access, such as escorted or granted.

- Temporary contractors should receive their credentials **daily**. They should fill out information on a contractor log sheet, sign in and out, and return their credentials each day before exiting the venue.
  - Temporary contractors' credentials should be clearly visible and presented to access-control personnel upon request.
- Temporary credentials can also be designed to expire and therefore do not need to be returned at the end of the day.

BEST PRACTICE

Depending on the vendor and organization, **all full-time and part-time employees, as well as full-time and temporary contractors, should complete a credential application** that contains the terms and conditions for using the credential, as well as pass a background check commensurate with their job functions, either conducted by the venue or a contracting company, prior to being issued a credential. Some positions may require an investigation of substance abuse history or a pre-employment credit report as part of the background check.

Non-Event Visitors including individuals not employed by the venue who are there for meetings, tours, etc., should be provided general or non-event parking, if available, close to an entrance designated as the visitor's entrance.

- If general or non-event parking is not available, then **the visitors' names should be on an approved parking list** for validation by access-control personnel.

- Prior to entering an access control area, visitors' **vehicles should be searched and parking passes/ window stickers issued**. For further guidance, refer to the venue's parking procedures.

Tour groups visiting the venue should always be accompanied by credentialed staff with designated escort privileges.

- **A visitor log sheet should be created** for the tour group.
- **A point of contact should be responsible for the group,** including organizing the tour, knowing who is touring the venue and when, and knowing how many people will be in the tour group.
- **An appropriate number of escorts should accompany the tour group** to ensure that the group stays together.

Deliveries should be scheduled and approved ahead of time by the appropriate point of contact (refer to the venue's delivery/shipment procedures). The names of drivers and other staff facilitating the delivery should be provided as well.

- Ensure that **all deliveries are made to designated areas**, such as loading docks, at the venue.
- Drivers should **present a government-issued photo ID** upon entering the venue.
- Drivers who make mail, concessions, or other routine deliveries, or who deliver items beyond the designated area, such as beyond a loading dock inside the access control area, **should be issued a credential in accordance with the procedures used for temporary contractors** and escorted during the delivery.
- **Any delivery vehicles left unattended should be evaluated through the venue's and organization's policies.**

2.3.1 Wi-Fi access

While performing official business, credentialed individuals may need Wi-Fi or other similar network access. Wi-Fi access should be granted for the minimum period necessary to accomplish any required tasks. Similar to venue or event access, those on the Wi-Fi network should not have access to other aspects of the network. This can be accomplished through network segmentation.

Some possible network segmentation options are:

- **Guest access** or an unrestricted, but separate, public access network.
- **Limited-time access** with a username and password that expire within a set timeframe or at the conclusion of an event.
- **Long-term Wi-Fi access** with assigned, individual usernames and accounts.

See the venue's information technology security polices for more information on credentialed individuals' access to network systems.

3 Credentialing Process

3.1 How to request a credential

A credential request form should be used to request all credentials.

This form should include the recipient's personal information as well as the credential's function, areas of access, timeframe, and terms and conditions. The form should also clearly state the penalties for violations of the credentialing program.

BEST PRACTICE

When possible, develop an online credential registration system to make the request process more efficient.

Event staff and attendees should complete and sign the form either online prior to the event or in person at the venue's credentialing office. Out-of-town individuals such as visiting teams, performers, friends and family, exhibitors, national sports league staff, media, and VIPs should submit credentialing requests electronically via fax, email, or online portal. These requests should be divided into categories or groups based on functions (e.g., concessions, ushers, visiting team, or event staff).

The point of contact for credentialing at the venue or event should be responsible for:

- **Granting or denying all requests for credentials** based on the guidance provided by the security manager responsible for the venue or event
- **Making the recommendation for approval or disapproval of a credential request** and providing this recommendation to the credentialing office for final processing.
- **Notifying the individuals requesting credentials of the action taken on their behalf** (either approved or denied) via email or postal mail. A formal justification for disapproval should be provided as well.

Develop written access criteria for each controlled area to support the approval or denial process.

In order to obtain a credential, an individual should appear in person at the credentialing office and present a valid government-issued photo ID, unless other arrangements have been made, such as a designated individual obtaining several credentials for a functional group. Note that the individual's name displayed on this photo ID must match the name on the credential.

The credentialing program should be flexible in order to coordinate venue-specific credentialing with the varied requirements of national touring groups, concerts, professional sports events, meetings of national associations, and other events. As an example, a professional sports league may issue season passes to the media, league staff, and the regular traveling party for each team. Season passes should contain a photo ID for quick identification purposes. Based on the agreements between the sports league and the venue, these season passes may allow the user access to all venues where the league holds events.

- **Integrate season passes** with the venue's specific credentialing program.
- The home team or venue should issue **day or event passes** in addition to season passes to determine levels of access and record attendance on an event-by-event basis.
- **A similar process can be employed for media personnel** who accompany a team on away games.

BEST PRACTICE
The venue should establish a maximum number of guest and/or family credentials allowed for team members, VIPs, and season-ticket holders with exceptions granted in special circumstances. Ensure VIPs, team members, and performers understand the importance of the venue's credentialing program and that abuses can result in the cancellation or reduction of the number of credentials issued.

All staff or guests of a venue must complete a security screening when receiving a credential. For more information on the aspects of a security screening, please see the security guidelines and procedures for the venue.

3.1.1 Supplemental credentials

For those instances in which access is required after a badge or credential has been issued, a supplemental credential, such as a colored wristband, upgrade chip or add-on credential can be issued to an individual for access to an event or area of the venue.

Escort privileges are only provided to specific credentialed individuals, such as full-time and part-time staff. Credentialed individuals may need to be escorted if they are accessing a restricted area beyond their allowed access. If credentialed staff have escort privileges, that should be indicated somewhere on the credential. If there are individuals who do not have credentials, they must be accompanied by an escort.

3.2 How to use a credential

Credentials should always be worn and clearly displayed on the outer layer of clothing within the controlled areas. **The possession of a credential does not negate security screenings**; even those with credentials are subject to all screenings and must follow all security procedures.

Train access-control personnel in recognizing the credentials that are allowed within their specific controlled area, identifying counterfeit credentials, understanding the procedures for denying entry, and confiscating credentials. There should be zero tolerance for allowing an individual into a controlled area without the proper credential. All venue staff should enforce the credentialing program and report abuses to venue security.

Develop specific procedures for access-control personnel and all venue employees to notify security of violations of the credentialing program.

3.2.1 Law enforcement

It is important for event and security staff to be able to identify all local law enforcement present at an event whether in uniform, in plain clothes, or undercover. Event organizers should also be able to distinguish those officers who are there on official duty and those who are not. Law enforcement officers should conform to the same credentialing requirements as all other event attendees: their credentials should be readily visible, include access marking, and be worn only during official business. If responding to an incident, plain-clothes and undercover officers should have an indicator on their credentials to clearly identify them as law enforcement officers to event security staff and other law enforcement personnel.

BEST PRACTICE
If the venue allows non-uniformed law enforcement personnel to enter the venue with a firearm, this should be indicated somewhere on the credential.

3.2.2 Talent

Because of their duties and job responsibilities at the venue, certain individuals, such as performers, players, and officials in uniform, should be the only persons not required to wear a credential. When not in a designated controlled area, these individuals must wear a credential to enter other controlled areas within the venue. Provide non-uniformed players with an event day credential to wear during the event.

A roster should be created that identifies the names and job responsibilities of the individuals who do not require credentials within specific controlled areas, including playing fields, racetracks, pit areas, or back of house. These individuals may enter the venue by way of a controlled, non-public access point, such as a team's and/or performer's parking lot. Individuals should be identified by a valid government-issued photo ID and confirmed by the roster.

Venues should consider assigning a security staff member to restricted performance areas, including team locker rooms and dressing or green rooms, to ensure that only approved persons are admitted. These approved individuals include players, coaches, credentialed team staff, and working media; all other persons should be denied entrance. Escorts should be provided when necessary.

3.3 How to verify a credential

Make sure to thoroughly check each credential prior to granting access. This includes touching and reviewing the credential, and if the credential has a photo, confirming that the credential holder is the person depicted in the image. For a name-only credential, the verifier may need to confirm the credential holder's identity by requesting a second valid ID, such as a driver's license. Lastly, credentials may also be verified through an electronic verification process that may include scanning a bar code or magnetic strip.

BEST PRACTICE

An example credential is highlighted below. This credential includes many of the security aspects detailed in previous sections, such as the event name, the location and dates for which this credential is valid, and other unique qualifiers that make this a secure credential.

FIGURE 1: AN EXAMPLE CREDENTIAL (IAFE)

3.4 What to do with expired credentials

An expired credential may pose a risk to a credentialing system.

Collect and destroy expired credentials to ensure they are not counterfeited or used improperly.

3.5 What to do with revoked credentials

A person with access to a revoked credential may pose a risk to the credentialing system and the venue.

Revoke a credential if it is worn offsite, during nonworking or non-event hours, or if its holder uses it to access areas unofficially.

For more information about consequences regarding the use of revoked or expired credentials and other related procedures, please review the security procedures for the venue.

4 When to Use Credentials

4.1 Non-event day procedures

On non-event days, access to the venue should be restricted to designated entrances based on job function, such as venue personnel, contractors, media, or event staff. Security and access-control personnel assigned to entrances should ensure that only those individuals displaying proper credentials for that access point are permitted entry.

BEST PRACTICE
Control access to sensitive areas of the venue, including information technology services, communications, finance, and electrical equipment, by using swipe card credentials and keys.

Thoroughly check each credential prior to granting access, using the methods outlined above in Section 3.3.

An organizational chart should be developed that identifies all roles and job responsibilities of non-event individuals, such as maintenance, engineering, or administration personnel.

- The timeframes needed to carry out these job responsibilities should also be identified; these include full-time, part-time, and event-specific schedules.
- The chart should also define areas of the venue where activities associated with roles and job responsibilities take place, such as part-time employees in the front office, full-time operations in engineering areas, or contracting work in the back office.
- Finally, the chart should identify the types of employees and their work status, whether full-time, part-time, event-specific, or otherwise.

If possible, consider creating daily spreadsheets from the credentialing system that list the credentials provided by function and venue location access, as well as to whom each credential was issued.

4.2 Event day procedures

Like the non-event day credentialing process, event day credentialing should be based on each individual's job function at the venue and areas of granted access. Unlike non-event days, access control is greatly expanded to include a wider range of job functions, as well as many categories of locations that might not be controlled during non-event days, such as locker rooms, operations and service areas, or press boxes.

Development of an organizational chart that identifies individuals' job functions, associated areas of access, and access restrictions during an event can help to enhance a credentialing scheme that reflects the desired access control during an event.

Credentials for employees should have a marking that **indicates if the credential is valid during event days**.

- **Full-time employees and contractors** may have credentials that are in effect year-round but may not be valid during event days.
- **Part-time employees** may have credentials that expire at the end of a contract, work order, or event season, such as a baseball season, concert, or theatrical series, but their job function may not permit them to use that credential during an event itself.
- **Event staff and participants** may have credentials that expire on a specific day during an event or that are valid throughout the entire event.

BEST PRACTICE

Access control points should have a "Sample Credential Board" that clearly identifies which credentials allow access to each entrance. This board should only be accessible by staff and should not be public to avoid the possibility of creating counterfeit credentials.

FIGURE 2: EXAMPLE CREDENTIAL BOARD (IAFE)

4.3 Post-event and event close-out procedures

Venues should employ the same level of concern for unauthorized entry into the venue after an event has ended while spectators or patrons are still present as they do for unauthorized entry before and during the event.

Adequate security and event staff members should remain present to deal with the large crowds all exiting the venue at one time; they should pay attention to those individuals wishing to enter or reenter the venue at the end of an event.

- Depending on venue and organization, **collect all temporary credentials** at all controlled access points Credentials can also be designed so that they expire and are disposable following an event.
- **Cross-check returned temporary credentials** to identify credentials not returned.
- **Destroy or deactivate credentials** that are expired or otherwise no longer valid.

5 Additional Resources

DHS and CISA provide a number of websites, videos, guides, and other resources that may be useful for those developing a credentialing program for public venues.

CISA Websites

Title	Link
Active Shooter Preparedness	https://www.cisa.gov/active-shooter-preparedness
Commercial Facilities Sector	https://www.cisa.gov/commercial-facilities-sector
Hometown Security	https://www.cisa.gov/hometown-security
If You See Something, Say Something®	https://www.dhs.gov/see-something-say-something

CISA Videos

Title	Link
No Reservations: Suspicious Behavior in Hotels	English: https://www.cisa.gov/video/no-reservations-suspicious-behavior-hotels Spanish: https://www.cisa.gov/video/sin-reservaciones-comportamiento-sospechoso-en-los-hoteles
What's in Store: Ordinary People, Extraordinary Events	https://www.cisa.gov/video/whats-store-ordinary-people-extraordinary-events

CISA Guides and Other Publications

Title	Link
Public Venue Bag Search Procedures Guide	https://www.cisa.gov/sites/default/files/publications/public_venue_bag_search_procedures_guide_3jun2019_v2_final_508.pdf
Security of Soft Targets and Crowded Places—Resource Guide	https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf
Patron Screening Best Practices Guide	https://www.cisa.gov/sites/default/files/publications/patron-screening-guide-03-16-508.pdf
Commercial Facilities Sector-Specific Plan, An Annex to the NIPP 2013	https://www.cisa.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf

6 Acknowledgements

The guide was developed by CISA in collaboration with the Commercial Facilities Sector Coordinating Council with representation from Public Assembly, Outdoor Events, and Sports Leagues Subsectors.

Additional input provided by:

Rick Brown
Regional/Branch Manager
Contemporary Services Corporation

Troy Brown
Vice President of Stadium Operations
Cleveland Browns

Marla Calico
President & CEO
International Associations of Fairs and Expositions

Mario Coutinho
Vice President, Stadium Operations & Security
Toronto Blue Jays Baseball Club & Rogers Centre

Christopher Davis
Vice President and Chief Security Officer
NASCAR

Mark Glaser
Senior Vice President, Operations
Contemporary Services Corporation

Andrea Grumet
Senior League Credentialist
National Basketball Association

Joe Levy
Executive Vice President, Deputy Director for Operations
National September 11 Memorial and Museum

Mary Mycka
Executive Director
Stadium Managers Association

Michael Rodriguez
Senior Director
USTA and US Open Security

William D. Squires
Founder/President
The Right Stuff Consulting, Inc.

David Thomas
Vice President, Security & Ballpark Operations
Office of the Commissioner, MLB

Photos for this guide were generously provided by the International Association of Fairs and Expositions (IAFE).

Please contact cfsteam@cisa.dhs.gov or visit https://www.cisa.gov/commercial-facilities-sector if you have questions or to find additional resources.


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY