January 8, 2018

Table of Contents:

Overview ............................................................................................................. 1
North Korea ......................................................................................................... 3
Crime ................................................................................................................. 4
Victim and Emergency Assistance .................................................................... 4
Protest Activity .................................................................................................... 6
Terrorism ............................................................................................................. 6
Host-nation Security Planning ............................................................................ 9
Information Security and Cyber Threats .......................................................... 9
Health and Medical ............................................................................................ 11
OSAC Support ................................................................................................... 13
Additional Resources ......................................................................................... 14
Maps ................................................................................................................... 15

OVERVIEW

The 2018 PyeongChang Winter Olympic and Paralympic Games will take place in the Republic of Korea (South Korea) from February 9-25 and March 9-18, respectively. Major events are often viewed as a potential platform for activists, protest organizations, and terrorist groups to amplify their message while the world is watching. Security for the Winter Olympic Games will be carried out by South Korean military and police forces, in conjunction with the PyeongChang Organizing Committee for the Olympic Games (POCOG). South Korea has a long history of successfully hosting major events, including the 2014 Asian Games, 2011 World Athletics Championships, 2002 FIFA World Cup, and 1988 Summer Olympics. The South Korean government has developed robust security and response plans, and has invested considerable resources into ensuring a safe and secure event. Authorities are continually monitoring for potential threats, and assess the risk of extremist activity, the possibility for demonstrations, and the likelihood of violent criminal incidents to be low.

The Olympics and Paralympics will bring together over 8,000 athletes from over 100 countries to compete in over 180 events. The competitions will be largely grouped into two clusters in the country’s eastern Gangwon province. Snow and sliding sports will take place in the mountain cluster in PyeongChang county, while ice events will occur in the coastal cluster in the city of Gangneung. PyeongChang, a popular hiking and skiing destination, is located more than 100 miles east of Seoul, while Gangneung, a popular summer beach destination, is located another 40 miles east of PyeongChang. (For detailed maps, see the Maps section of this report.)
One of the primary infrastructure projects for the Olympic Games has been the extension of the KTX high-speed rail line, which as of January 2018 connects the west coast’s Incheon International Airport (ICN) to the east coast’s city of Gangneung. The new 278-kilometer line significantly decreases the travel time from Seoul to PyeongChang and Gangneung. A three-hour drive from Seoul to PyeongChang will take approximately one hour and 20 minutes on the high-speed train. From PyeongChang in the mountain cluster to Gangneung in the coastal cluster will take another 20 minutes. During the Games, 102 trains (51 roundtrips) will operate daily with a total capacity of over 40,000 passengers, which does not include standing passengers who are also permitted on these trains. Free spectator shuttle buses will be provided from the Jinbu and Gangneung KTX stations to the Olympic venues. Additional train and transportation information can be located on the official Olympic Games website and the KORAIL website.
Travelers are advised to pay particular attention to the names of the train stations providing access to the Games. For example, the primary KTX train station for travel to the Olympic Games from Seoul is Cheongnyangni station, not Seoul station. Cheongnyangni station will have 43 trains per day traveling from Seoul to the Olympic clusters whereas the Seoul station will have only 8 trains. Additionally, the primary train station closest to most Olympic venues in the mountain cluster is Jinbu station (not PyeongChang station).

NORTH KOREA

Much of the media reporting in the lead-up to the 2018 Winter Games has focused on the perceived threat from North Korea, in part due to its relative proximity to the Olympic venues and to the South Korean capital of Seoul. OSAC, however, is not aware of any specific, credible threats to Olympic events, athletes, staff, sponsors, or attendees from North Korea, and has not seen any evidence to suggest that any such threats are forthcoming. If OSAC or the U.S. Embassy in Seoul becomes aware of any specific and credible threats to the safety and security of U.S. citizens and/or OSAC constituent organizations, such information will be provided on OSAC.gov and the U.S. Embassy website, as well as via social media and email. (More information on Host-nation Security Planning and Emergency Assistance can be found in the respective sections of this report.)

The U.S. Embassy in Seoul continues to engage in its routine course of business and there have been no changes to its security posture, levels of staffing, or the guidance issued to American citizens living in or traveling to South Korea. In December 2017, a spokesman for the U.S. Olympic Committee (USOC) confirmed that the U.S. would be sending two full delegations to the Olympics and Paralympics, adding that USOC had not had any discussions, either internally or with government partners, about not participating in the Games. OSAC is not aware of any U.S. private sector organizations operating in Korea that have significantly changed their respective operations at the Olympics/Paralympics as a result of security considerations, but some organizations have opted for a reduced footprint.

U.S. private-sector organizations are advised to continue monitoring the security situation on the Korean Peninsula through official U.S. government messaging and local media. This includes identifying trustworthy sources of information and verifying reports that lack credible sourcing – as misinformation and sensational reporting are likely to be present in the lead up to and throughout the Games. To address these and other concerns, OSAC will be fielding a team of analysts that will participate in an interagency, 24-hour Joint Operations Center run out of U.S. Embassy Seoul. In that role, OSAC will work with other U.S. Government offices, Olympic sponsors, and host-nation authorities to share timely and accurate security information with the U.S. private sector, including through the issuance of a daily, unclassified situational report of events on the ground. (To be added to the report's distribution list see the OSAC Support section of this report.)

Background: An armistice agreement signed in 1953 has generally served to maintain peace between the Republic of Korea (South Korea) and the Democratic People’s Republic of Korea (North Korea). Bilateral tensions on the Korean Peninsula remain moderately high and are periodically marked by incendiary rhetoric and provocative actions from the North.

Many of these provocations involve North Korea’s continued testing of nuclear and ballistic missile technology. North Korea is believed to have tested approximately two dozen missiles in 2017 alone, including what were believed to be the country’s first intercontinental ballistic missiles (ICBMs), as well as shorter-range missiles that traversed Japanese airspace. In September, North Korea conducted its sixth controlled nuclear device detonation, which resulted in the country’s largest explosive yield to date.

North Korea has also been responsible for limited armed incursions into South Korean-held territory and geographically-confined military skirmishes. These include the unprovoked sinking of a South Korean naval vessel and the shelling of a South Korean island in 2010. As recently as August 2015, North and
South Korea were briefly engaged in the exchange of artillery across the Demilitarized Zone (DMZ) separating the two countries.

Provocations such as these have resulted in multiple rounds of UN Security Council sanctions against North Korea, designed to cut off sources of revenue used to fund the country's nuclear and ballistic missile programs. These sanctions often result in incendiary rhetoric from North Korea, such as threats to make the U.S. experience "great pain" for leading the sanctions efforts.

Similarly, North Korea has historically issued strongly-worded threats in response to joint U.S. and South Korean military training exercises, particularly those held annually in the spring and fall. U.S. and South Korean authorities have agreed to re-schedule the Key Resolve and Foal Eagle exercises – which typically take place in late February/early March – until after the conclusion of the Paralympic Games. This decision was made to de-conflict the timing of the Olympics and military exercises so that U.S. and South Korean forces could focus on ensuring the security of the Games.

CRIME

Crime in South Korea is typically non-violent and involves petty property theft, such as pick-pocketing, purse snatching, and thefts from hotel rooms. This type of crime occurs more frequently in major metropolitan areas, at tourist attractions, and in crowded venues. Though less common, there have been reports of sexual assault committed against foreigners; reporting has shown that the majority of reported sexual assault cases involved alcohol. While most crimes are typically non-confrontational, violent crimes do occur and sometimes involve the use of knives; firearms are very uncommon due to stringent gun control laws.

According to the Korean National Policy Agency (KNPA) and the Justice Ministry, during the Olympic Games a broad set of measures will be enforced by police to curb crimes. Police investigators and immigration officials will step up patrols and inspections in seven major areas near Olympic venues, including the Olympic Plaza in PyeongChang and the Gyeongpodae area of Gangneung, to deter criminal activity and to respond to any incidents that may occur.

U.S. citizens attending the Winter Olympic Games should exercise caution in all crowded venues and areas, and it is advised to avoid carrying valuables in backpacks, which are more easily targeted by pickpockets. Visitors should also maintain situational awareness while at entertainment, nightlife, and shopping districts (especially in the Itaewon, Sinchon, Myeongdong, Gangnam, and Hongdae areas of Seoul), as crowds, alcohol, and a higher prevalence of drug activity present a higher risk of crime.

VICTIM AND EMERGENCY ASSISTANCE

Victim Assistance: Travelers should call the police emergency telephone number 112 if they are the victim of a crime or need police assistance. Officers with English-speaking capability are on duty at all times. U.S. citizens are also encouraged to report the crime to the American Citizen Services section of U.S. Embassy Seoul by calling (+82-2) 397-4114. (To make calls within South Korea using a phone with a U.S.-based SIM card, one needs to first dial +82, followed by the area code – 2 is the area code for Seoul – before the phone number.)

Police: 112
Medical/Fire/Emergency: 119

Other Assistance: South Korean authorities have established an Olympics Information Call Center. Travelers can dial 1330 to receive and report information about the Winter Games. According to the official PyeongChang Olympic Games website, callers can ask about tourism tips, report complaints, request interpretation service, as well as receive assistance on accommodation reservations, restaurants,
transportation, cultural events, and other items related to the Winter Games. The call center is able to provide Korean-, English-, Japanese-, and Chinese-language services.

**Emergency Communications, Notification Systems, and Shelters:** The South Korean government manages a nation-wide warning system to notify the public during emergencies. Alarms are sent simultaneously through TV, radio, and loudspeakers.

<table>
<thead>
<tr>
<th>Warning Alarm</th>
<th>Enemy attack is anticipated</th>
<th>1-minute</th>
<th>flat tone (———)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air-raid Alarm</td>
<td>Enemy attack has commenced</td>
<td>3-minute</td>
<td>wave tone (~~~)</td>
</tr>
</tbody>
</table>

More information on distinguishing emergency sirens can be found within the publically available [Emergency Ready mobile application](#). Korean cell phone subscribers should also receive automatic Emergency Alert SMS messages, though these have historically been available exclusively in Korean. Recent examples of these messages have involved updates on severe weather.

According to the “[Emergency Procedures Manual for Foreigners](#),” published by the South Korean Ministry of Security and Public Administration and the Ministry of Foreign Affairs, there are 24,000 public shelters across South Korea, including more than 3,000 in greater Seoul. Most of these shelters (alternatively referred to as civilian defense facilities) are multi-purpose structures, such as subway stations, underground parking lots, and building basements.

- Shelters are designated by the icon pictured on the right.
- Shelters can also be identified in advance using the [Emergency Ready app](#).
- For a general idea of the location of shelters throughout metro Seoul, Reuters produced a visualization in May 2017, which can be found [here](#).
- In the event of an emergency warning, individuals are advised to follow instructions and control from Civil Defense personnel wearing yellow hats and jackets with a civil defense symbol.

Additional resources:

- [ROK Ministry of Foreign Affairs Twitter](#)
- [ROK National Fire Agency Twitter](#) (which re-tweets most domestic emergency notifications)
- [ROK Meteorological Administration website](#) (which can potentially be used to confirm weather-related emergencies)

Emergency guidance will also likely be pushed out by the U.S. Embassy in Seoul via the following means:

- [U.S. Embassy Seoul Safety & Security Messages](#)
- [U.S. Embassy Seoul Disaster Preparedness Webpage](#)
- [U.S. Embassy Seoul Twitter](#)
- [Travel.State.Gov Korea Country Information page](#)

American Forces Network (AFN) Korea radio channels may also provide guidance in the case of a natural disaster or civil emergency.

- There are no AFN stations in Gangwon province; the closest stations are via Chuncheon (88.5 FM / 1440 AM) and Wonju (88.3 FM / 1440 AM).
- The station for Seoul is 102.7 FM / 1530 AM.
- A complete list of AFN stations by locality can be found using the [AFN Pacific mobile app](#).
PROTEST ACTIVITY

Freedom of assembly is protected by Korean law and the right to protest is regularly exercised throughout the country. Public demonstrations are a routine occurrence and most are peaceful and well-policied. Due to the frequency of demonstrations, the U.S. Embassy closely monitors and assesses each event and will issue alerts to the American community when deemed appropriate; a total of four such alerts were disseminated in 2017.

Rallies are frequently held in central Seoul near the U.S. Embassy and Seoul City Hall. In 2017, the U.S. deployment of the Terminal High Altitude Area Defense (THAAD) anti-missile system on South Korean territory led to several anti-U.S. government protests.

Though most public demonstrations in South Korea are peaceful, there have been clashes between the police and protesters where non-lethal tactics were employed to manage disruptive crowds, including the use of water cannons, tear gas, and police bus barricades to cordon off restricted areas. Demonstrations though are more likely to disrupt traffic than spark a clash between police and protestors. The Korean National Police Agency (KNPA) maintains the right to place limits on assembly if the demonstration is to undermine public order or spark violence, but the enforcement of limiting protests is uncommon.

Korean protest organizers coordinate with law enforcement officials to conduct hundreds of protests each year. As a precaution, however, OSAC constituents should avoid areas where demonstrations are taking place and exercise caution in the vicinity of any large gatherings, protests, or rallies. Even demonstrations intended to be peaceful can turn confrontational and escalate into violence. Moreover, foreign visitors are prohibited from participating in political demonstrations in South Korea because doing so would violate the terms of their visa.

In the past, the Olympic Games have been perceived as an attractive platform for activists to amplify their messages to a larger audience. At this time, OSAC is not aware of any Olympics-specific protests planned for during the Games. As the event draws closer, it is possible that protests will materialize. Several current factors, however, suggest that this activity will be limited.

For one, the vast majority of large-scale protests occur in Seoul. While some OSAC constituents will have Olympics-related operations in the capital, most will be located in PyeongChang, Gangneung, and other areas of Gangwon province that are not pre-disposed to protest activity.

Additionally, in the lead up to the Games, no significant anti-Olympics movement has emerged in the country. The Games are not mired in political controversy and have generally enjoyed high public approval ratings. Political protests both against and in support of former President Park have waned following her impeachment in December 2016 and removal from office in March 2017.

Finally, South Korea’s cold winter months of February and March tend to discourage large demonstrations and rallies.

TERRORISM

OSAC is not aware of any specific, credible terrorist threats targeting the 2018 Winter Olympic Games. There has not been a terrorist incident directed against American interests in South Korea in recent history, and the threat of terrorism throughout the country is generally considered low. There are no known domestic or transnational terrorist organizations present in South Korea; however, the possibility of a homegrown, self-radicalized “lone offender” conducting an attack cannot be ruled out. International sporting events can offer radicalized individuals and extremist groups an attractive target for a high-profile attack.
Korean authorities are continually monitoring for potential threats. In December 2017, South Korea deported 17 foreigners in a preemptive anti-terrorism action. The individuals were never publically identified but according to the Korean Immigration Service they included nationals from at least five countries in Southeast and Central Asia. While no specific terrorist plot was revealed, authorities stated that the individuals were deported for being members of international terrorist groups as defined by South Korea’s anti-terrorism law or were on the terrorist watchlists of partner nations.

Additionally, also in December, the government conducted a series of security drills at the Olympic Stadium in PyeongChang. By simulating terrorist attack scenarios, including a mock drone attack, a hostage situation, and a vehicle attack, authorities are likely better positioned to respond to various incidents and to identify potential vulnerabilities within existing counter-terrorism plans.

Countermeasures implemented by South Korean authorities include vehicle bollards to limit the possibility of vehicle attacks. Additionally, two meter-high secure perimeter fences have been constructed at every venue. Regarding access to weapons, stringent gun control laws are likely to prevent most would-be attackers from acquiring firearms.

In November 2017, citing threats of “nuclear devastation” and “acts of international terrorism, including assassinations on foreign soil,” the U.S. Department of State re-designated North Korea as a state sponsor of terrorism. (North Korea had previously been designated a state-sponsor of terrorism from 1988-2008.) The Olympic competition venues are located approximately 50 miles from the border with the DPRK. Though North Korea’s provocative behavior in 2017 has elevated tensions on the Peninsula, the likelihood of an attack conducted by a state actor, such as the DPRK, during the Games is assessed to be low.

HOST-NATION SECURITY PLANNING

To protect tens of thousands of tourists and athletes, the Korean Defense Ministry plans to deploy over 5,000 security agents, as well as 1,000 contract security personnel to the Winter Games. Moreover, the Korean National Police Agency reports that they plan to mobilize a force of approximately 137,000 police officers during the Games. While security personnel numbers may fluctuate slightly as the Games progress, they are expected to remain sufficient throughout the entirety of the events. The Counter-Terrorism Safety and Security Center (CSSC) and the Organizing Committee’s Security Bureau (POCOG) are the primary entities responsible for security planning at the Olympic venues. The agencies listed below will contribute and implement the government’s security plan for the Games.

**Counter-Terrorism Safety and Security Center (CSSC):** The CSSC is a temporary organization comprised of 19 different government ministries and other institutions directly involved in counter-terrorism and law enforcement. In preparation for the Winter Games, the CSSC is responsible for overseeing all counter-terrorism and security threats, risks, and response measures. During the Games, it will be the head of all operations, delegating tasks to subordinate bodies and monitoring all activities from its two field command centers in PyeongChang and Gangneung.

**Ministry of National Defense (MND):** MND elements will be responsible for providing security of regions outside the Games facilities, as well as maritime and airspace jurisdiction. The Defense Ministry plans to deploy over 5,000 security agents to the Games, as well as 1,000 contract security personnel.

**National Intelligence Service (NIS):** The NIS is the domestic and foreign intelligence service, but it also has a quasi-law enforcement function. Its Threat Information Integration Center is responsible for counter-terrorism activities and security planning for major international events. NIS has the lead in coordinating all intelligence threat streams for the Olympic Games.

**National Police Agency (KNPA):** The KNPA is the national police force. Its responsibilities include criminal investigations, public safety, cybersecurity, traffic, counterterrorism, riot control, and dignitary
protection. KNPA officers will provide traffic control for all Games venues and access roads, will support security and access control of Games facilities, and will provide personal protection for athletes and foreign dignitaries. KNPA elements are also responsible for responding to reports of petty and violent criminal incidents.

- **Combat Police**: An anti-riot paramilitary unit of military conscripts. Its members deal with counterintelligence and riot policing. The Combat Police are deployed at demonstrations and rallies where violent disorder may occur.

- **Special Weapons and Tactics (SWAT)**: KNPA’s SWAT unit is the premier civilian authority charged with counterterrorism operations and is responsible for serving high-risk arrest warrants, hostage rescue, and other high threat missions. The SWAT teams are considered well-equipped, well-organized, and well-trained.

- **Tourist Police**: In 2013, the KNPA created a tourist police unit that is responsible for patrolling major tourist areas in Seoul and whose officers are fluent in English, Japanese, and Mandarin. Tourist police officers will be assigned to venues in PyeongChang and Gangneung to assist visitors during the Games.

**Presidential Security Service (PSS)**: PSS is an independent agency responsible for the protection of the South Korean President and his family, the official residence of the head of state, visiting heads of state, and any other domestic and/or foreign persons deemed necessary. PSS implements security guard activities for special events, including the Opening and Closing Ceremonies of the Olympic and Paralympic Games. PSS will also be providing personal protection for designated VIPs attending the Games.

**Ministry of Public Safety and Security (MPSS) Fire Department**: MPSS officers are responsible for fire prevention and extinguishment, as well as the transfer of injured athletes and spectators to relevant medical facilities.

**Private Security**: POCOG has hired UNIES, a private security contractor that currently provides security services to Incheon International Airport, stipulating the firm should be capable of running approximately 500 personnel to operate access control screening technology during the Games.

**Securing Venues and Soft Targets**

POCOG and KNPA police elements will provide internal venue security at the Games. Private security, police, and volunteer elements are responsible for maintaining access control to the venues, and KNPA, PSS, and military officers are responsible for patrolling and maintaining public order on the outside security perimeters of all venues. Pedestrian Screening Areas (PSA) and Vehicle Screening Areas (VSA) will be operated jointly by KNPA elements and private security elements to prevent prohibited items from coming into the venues. Strict accreditation checks will be performed at these entrance points as well.

Venue Security Control Centers (VSCCs) – joint operations centers comprised of POCOG and various Korean defense, law enforcement, and intelligence agencies – will be established at every venue. The VSCCs are responsible for control management of the private security workforce and monitoring the overall security situation of the venues, to include preventing public disorder.

Additionally, venue airspace has been designated as “no-fly” zones during the Games for unauthorized flying objects such as unmanned aerial vehicles, air balloons, helicopters, and other aircraft. A traffic management center will be established to relieve traffic congestion, while a police service center and a lost & found service will assist with missing items at venues.
The Organizing Committee has recognized the challenge presented by soft targets, such as fan parks, hotels, restaurants, hospitality sites, transportation locations, and other tourist attractions. Security forces have conducted several drills and crisis management exercises in anticipation of a variety of security scenarios. As part of the drills, KNPA’s SWAT unit has practiced shooting down a bomb-carrying drone headed for a bus full of athletes and gunning down a person hijacking a bus and attempting to ram it into the stadium. Officers also practiced removing a chemical bomb. While it is believed that these enhanced security measures will adequately address the threat, OSAC constituents should remain vigilant and aware of their surroundings at all times, especially in crowded areas.

**INFORMATION SECURITY AND CYBER THREATS**

Major events are attractive targets for nation-state, criminal, and “hacktivist” cyber threat actors. OSAC constituent websites, networks, electronic devices, and sensitive information have been targeted during past major events. Cyberattack technologies, including surveillance, economic espionage, distributed-denial-of-service, and cybercrime capabilities are prevalent in South Korea.

In December 2017, McAfee, a cyber security company, discovered a hacking campaign that targeted organizations involved in the PyeongChang Winter Games. According to their report, “The majority of these organizations (targeted) had some association with the Olympics, either in providing infrastructure or in a supporting role.” Targets were sent an email purporting to be from South Korea’s National Counter-Terrorism Center but the spoofed emails came from an address in Singapore and instructed the readers to open a text document in Korean. The hackers used a more sophisticated method than the average “spear phishing” attack by installing malicious software without making the victim download a file, which is often flagged by a security program. The malware in some cases was hidden in text, and later in an image, a method not previously seen targeting victims in South Korea.

South Korean authorities are cognizant of the possibility of a hacking attack from North Korea during the Olympics/Paralympics, whose cyber army has previously targeted foreign companies and South Korean private and public institutions. POCOG has selected a team of private-sector cybersecurity professionals to upgrade its cyber defenses and guard against possible intrusions during the Games.

North Korea poses a particularly significant threat to South Korean cybersecurity. South Korea has blamed North Korea for a series of hacking attempts over the past several years. Since 2009, North Korea’s army of more than 6,000 hackers – referred to collectively by industry experts as “HIDDEN COBRA,” “Lazarus Group,” and “Guardians of Peace” – have successfully performed dozens of network intrusions. Several high-profile targeted cyber espionage operations have been observed in South Korea, most of which are attributed to North Korea. These attacks have resulted in the theft of millions of dollars, the exfiltration of highly sensitive data, and the disruption of critical operations. Victims of malicious North Korean cyber activity have included international financial institutions, private-sector media and entertainment organizations, defense and aerospace industries, think tanks and research institutions, and critical infrastructure systems.

U.S. private sector organizations operating globally remain vulnerable to North Korean cyber actors. In December 2017, the U.S. Government officially attributed the massive 2017 “WannaCry” cyberattack to North Korean actors. WannaCry, a computer worm paired with ransomware, encrypted computers and rendered them unusable until a ransom was paid. North Korea-affiliated agents were also detected attempting to phish U.S. electric companies through emails sent in September 2017. These incidents underscore an ongoing trend in which actors suspected of association with the North Korean government have persistently leveraged their cyber capabilities to advance the country’s strategic and military objectives, often at the expense of U.S. private-sector organizations.
Countermeasures

In December 2017, OSAC released a report entitled “Mitigating North Korean Cyber Threats,” outlining a list of best practices for mitigating potential threats from North Korea and other state-sponsors of malicious cyber activity. While a comprehensive cyber-security response plan is beyond the scope of this report, there are a number of simple countermeasures that private-sector security professionals can share with their staff and guests in order to reduce their organization’s vulnerability during the Olympic Games.

Routinely update and patch all software and operating systems, particularly with programs that have known vulnerabilities: Malicious cyber actors suspected of association with North Korea commonly target systems that are vulnerable to exploitation, such as older or unpatched versions of Microsoft operating systems, Adobe Flash Player, and Hangul Word Processor. According to media reports, Microsoft issued a patch for the software flaw that enabled WannaCry two months before the May 2017 attack, but many companies around the world failed to update their machines and fell victim to the crisis. Pirated software – including that used by third parties who constitute part of an organization’s business chain – may be particularly vulnerable, as applications and operating systems without authentic product keys may not be eligible for routine updates.

Exercise caution and learn to identify spear-phishing attempts: Malware samples suspected of being associated with North Korean cyber threat actors are thought to have been spread through spear-phishing email messages. Certain indicators may signal a heightened likelihood that an email is a spear-phishing attempt.

- **Look for red flags such as misspelled words or poor grammar.** An attack against the New York Federal Reserve last year was reportedly stopped due to a spelling error. In another instance, bankers at the Bangladesh Central Bank were initially suspicious when a withdrawal request misspelled “foundation” as “fandation;” ultimately, however, the typo was dismissed and suspected North Korean hackers were able to successfully steal $81 million.

- **Consider the relevance of the email, content, and sender.** Malicious cyber actors may create fake domains designed to spoof the user into believing they are legitimate. For example, hackers may send an email from “…@stategov.com” in order to mimic the actual domain “…@state.gov.” Private-sector professionals are also advised to confirm that the subject and content of the email is pertinent to all parties involved.

It is worth noting, however, that malicious cyber actors have become increasingly adept at using social engineering to learn more about specific spear-phishing targets and are tailoring their messages to seem directly relevant to the recipient. Often this information can be gleaned from a user’s online footprint and/or social media presence, underscoring the importance of operational security practices that limit the sharing of personal information and details.

- **Confirm that links lead to the intended website and have not been altered.** It is easy for hackers to edit the destination of a hyperlink, while leaving the language in the link unchanged. By hovering the cursor over a link, the user will be able to see the true destination, without actually accessing the link. Users should be wary of instances in which the text and the URL do not appear to have a logical relationship.

- **Manually navigate to the website by inputting the desired URL into the web browser, instead of clicking on the link directly.** Typing in the web address manually may prevent users from being unknowingly re-directed to an unintended website.

Exercise caution when downloading attachments and while running executable files: Malware suspected of ties to North Korea has been delivered through malicious decoy documents. When possible, all attachments should be scanned for malware. Additionally, some organizations may decide to limit the privileges of non-admin users so that they cannot run executable files (e.g., those ending in .exe and .dwg). The installation of such files could potentially result in the transfer of malware onto an organization’s network.
Use two-factor authentication for all accounts where possible: Two-factor authentication acts as a second layer of security to prevent an actor from gaining access to an account in the event of a compromised password. Private-sector security professionals are also encouraged to set up notifications for authentications and to regularly check login records for suspicious log-in attempts.

Confirm URL of websites, especially those requiring credentials: Hackers have demonstrated the ability to create convincing imitation websites in order to push malware and/or collect account information like usernames and passwords. Moreover, providing credentials to a malicious imitation website can be particularly problematic if the same username and password are also used on other sites, which may allow hackers access to more sensitive data and information.

Private-sector security professionals should also be wary of prompts encouraging them to reset their passwords or update their software while traveling or operating overseas. If prompted to reset one’s password, the user should verify that the URL of the re-direct page is associated with the account in question. Alternatively, and perhaps more cautiously, the user may consider accessing the password reset prompt directly through the service’s website, rather than through a link provided via email.

Other Considerations

Past major events have also served as lures in cyber espionage campaigns; malicious actors were observed using the schedule for previous Olympic Games as content for spear phishing messages. Cyber espionage campaigns are focused on gathering information for political or economic gain, and it is possible that malicious state actors could attempt to exploit South Korean and U.S. private sector organizations during the Games.

OSAC constituents should also be mindful of network infrastructure vulnerabilities, especially when connecting to public access points. Public Wi-Fi does not require authentication and easily enables malicious cyber actors to monitor traffic or to distribute malware. OSAC recommends refraining from or being wary of sensitive transactions or communications over unfamiliar or potentially insecure networks, such as internet cafes, hotel internet services, public hotspots in lobbies or airports, or leased equipment. Using a virtual private network (VPN) to access business information, and limiting logins of personal email, social media, and financial accounts can reduce the risk of information theft over public access points. If users find it necessary to access data from a public Wi-Fi network, constituents should consider these tips to help maintain data security and employ best practices while traveling.

Email and website scams have also leveraged past Olympic Games; cybercriminals have capitalized on the popularity of the event to spread malware or entice users into providing personal or financial information. Although not as prevalent in South Korea leading up to the Games, OSAC constituents should be aware of the possibility of fake ticketing services, where cybercriminals register website domains containing similar search terms to appear legitimate and mimic ticket vendors. To prevent counterfeit issues, all tickets at the Games will be encrypted with a QR code and hologram, as well as the full name of the original purchaser. The official website of the Olympic Games provides a list of certified ticket sellers and enables users to verify the legitimacy of event-related websites.

HEALTH AND MEDICAL

South Korea’s health care system is robust. Hospitals and clinics in South Korea are generally equipped with the latest medical diagnostic and therapeutic equipment, and the quality of medical service is similar to Western-style care in major metropolitan areas such as Seoul, Busan, Daegu, and other larger cities. Although not all doctors and staff are proficient in English, particularly in less tourist-prone areas, many medical facilities in the Olympic venue areas are opening “Foreigner Clinics” and increasing their multilingual staff during the Winter Games. As a resource for travelers, U.S. Embassy Seoul maintains a list of hospitals and medical specialists who speak English (mostly in Seoul) on its website.
**Medical Care and Emergencies:** South Korea has a professional emergency response capability that can quickly transport patients to the nearest hospital. To request an ambulance, dial 119. Managed by the National Emergency Management Office inside the Ministry of Interior and Safety, South Korea’s 119 emergency telephone system provides patient care and transport.

Eleven treatment clinics will be available at the Olympic venues for spectators to utilize. These clinics will have access to Automated External Defibrillators (AED) and EMT-level care. Patients requiring further care will be transported to one of two Olympic-approved hospitals for onward treatment: Wonju Severance Hospital, which is about half way from Gangneung and Seoul, or Gangneung Asan Hospital which is the closest facility to the coastal cluster. In addition to the regular ambulances requested through the country’s 119 emergency service, POCOG has secured additional Olympics-dedicated emergency ambulances. These POCOG ambulances will only transport patients to the POCOG approved hospitals, Wonju Severance Hospital and Gangneung Asan Hospital.

South Korea’s 119 emergency services are robust in Seoul and will provide ample response capabilities for events occurring outside the Olympics competition areas.

**Medical Bills and Insurance Coverage:** Travelers should verify their health insurance coverage before visiting South Korea. In most cases, health care providers will require payment in advance of treatment or will not release a patient until hospital bills are paid. Some hospitals accept a limited amount of American medical insurance, but only a few have negotiated direct-billing procedures. Further, hospitals – including emergency rooms – will not routinely admit foreigners as patients without payment (or verification of medical coverage) up front. OSAC strongly recommends constituents purchase supplemental traveler's medical insurance to include coverage for medical evacuation.

**Medication and Pharmacies:** Pharmacies in South Korea are very good and stock many common prescription and over-the-counter medicines. OSAC constituents should carry prescription medication in its original packaging – along with the doctor’s prescription note. Most prescriptions can be procured (except psychotropic types) at Korean pharmacies, though brand names may differ. Local pharmacies will require a prescription from a Korean doctor, thus, prescriptions will not be refilled at a local pharmacy without a local prescription.

Over-the-counter drugs (e.g., antihistamines, antacids, and vitamins) can be purchased at pharmacies without a prescription. However, specialized drugs like antibiotics will require a prescription. For additional information on controlled substances, or specialized prescriptions, visit U.S. Embassy Seoul’s webpage.

**Vaccinations:** The Centers for Disease Control and Prevention (CDC) recommends travelers are up-to-date on routine vaccines before traveling. These vaccines include measles-mumps-rubella (MMR), diphtheria-tetanus-pertussis, varicella (chickenpox), polio, and an annual flu shot. Further, the CDC recommends receiving the Hepatitis A vaccine due to the risk of contaminated food or water in South Korea, and the Typhoid vaccine especially if you are staying in smaller cities or rural areas.

Certain travelers are also recommended to receive the following vaccinations or medicines depending on their destinations in South Korea, what they will be doing, and if they are traveling from another country other than the United States: Hepatitis B, Japanese Encephalitis, Malaria, and Rabies. Visit the CDC webpage on South Korea as well as their Olympics-specific watch level page for verification and further recommendations.

**Food and Water:** Food sanitation is, for the most part, on par with U.S. standards. Caution should be taken when eating at small street vendors, however. Local city water is potable, though most Koreans drink bottled, boiled, or purified water. Most travelers do not need to take special food or water precautions beyond what they normally do at home.

**Additional Considerations:** Very cold temperatures and water can be dangerous, and steps to prevent hypothermia and frostbite should be taken. Travelers should dress in layers and cover head, hands, and
feet properly; avoid activities that would cause profuse sweating as wet clothing and cold weather can cause the body to lose heat more quickly; and to stay dry by getting out of wet clothing as quickly as possible. Prolonged exposure to cold temperatures can have irreversible and life-threatening effects. Individuals should protect themselves from UV radiation by applying sunscreen with an SPF of at least 15. Sunlight reflects off snow and water, and UV light is more intense at higher altitudes.

**OSAC SUPPORT**

OSAC will have five analysts based out of U.S. Embassy Seoul from February 7 to February 26 to support the U.S. private sector during the Winter Olympics. In addition to being available for phone/email/in-person consultations, the analysts will produce daily reports during the Olympics to keep constituents apprised of relevant security and logistical issues.

If you would like to be included on OSAC’s distribution list to receive daily reports related to the Games, please send a request to OSACMajorEvents@state.gov with your name, title, organization, contact details, and briefly state your organization’s footprint on the ground (e.g. Olympics-specific operations, regular business operations in South Korea, monitoring remotely for situational awareness, etc.).

Local phone numbers for OSAC support will be provided to the distribution list as soon as they are available.

For previous, relevant OSAC reporting, please see the following:

- OSAC Report: Between Chaos & Complacency on the Korean Peninsula
- OSAC Report: Mitigating North Korean Cyber Threats
- OSAC Report: North Korea Geographical Travel Restriction
- OSAC Report: North Korea’s Provocations & the Private-sector Response
- OSAC Report: Korean Peninsula Survey Results
- OSAC Report: North Korea’s Latest Missile Launch
- OSAC 2017 South Korea Crime and Safety Report

**American Citizen Services**

The U.S. Department of State recommends that all travelers enroll in the Smart Traveler Enrollment Program (STEP) prior to traveling overseas.

In addition to an updated Country Specific Information page, the State Department has developed several printed and electronic resources to assist private U.S. citizens visiting or resident in South Korea during the Olympic Games, including a printable Olympics Handout Card and a special webpage on the Embassy’s website. American citizens can also avail themselves of information by following U.S. Embassy Seoul's Facebook page, U.S. Embassy Seoul's “Americans in Korea” Facebook page, and U.S. Embassy Seoul’s Twitter feed.

U.S. Embassy Seoul
188 Sejong-daero, Jongno-gu, Seoul, Republic of Korea
Hours: Mon-Fri: 0800-1700 (except U.S. and Korean holidays)

Embassy Switchboard: +82-2-397-4114
American Citizen Services (ACS): seoulinfoacs@state.gov and +82-2-397-4040
After-hours Emergencies involving U.S. citizens: +82-2-397-4114
ADDITIONAL RESOURCES

U.S. Department of State:

- U.S. Embassy Seoul: Safety and Security Messages
- Consular Affairs: South Korea Country Information Page
- Consular Affairs: Olympics Webpage

Government of South Korea:

- Emergency Procedures Manual for Foreigners
- Ministry of the Interior and Safety (English)
- Korean Meteorological Administration Notices
- Korea’s National Fire Agency Twitter Feed (includes most emergency notifications)

South Korean English-language media:

- Chosun Ilbo
- Yonhap News Agency
- Dong-a Ilbo
- Korea JoongAng Daily

Helpful English-language apps: (links are for apps in the iTunes store)

- Emergency Ready (allows users to search for nearby shelters, access emergency tutorials, distinguish emergency sirens, etc.)
- Naver Map (maps, since many U.S. mapping apps do not have full-access to Korean data)
- Daum Map (another maps app)
- Subway (subway maps with real-time transit info, timetable, transfer info, station/area guide, etc.)
- Korean Dictionary & Translate (English to Korean dictionary/translation app)
- Visit Korea (developed by the Korea Tourism Organization, app includes information on exchange rates, maps, and emergency contact numbers)
- AFN Pacific (app allows anyone in Korea access to all of the available American Forces Network radio stations in the Pacific Region)

The contents of this unclassified report in no way represent the policies, views, or attitudes of the United States Department of State, or the United States Government, except as otherwise noted (e.g., travel advisories, public statements). The report was compiled from various open sources and unclassified government reporting. Please note that all OSAC products are for internal U.S. private sector security purposes only. Publishing or otherwise distributing OSAC-derived information in a manner inconsistent with this policy may result in the discontinuation of OSAC support.
Olympic Region Overview

- Gangneung Coastal Cluster
- PyeongChang Mountain Cluster
- Phoenix Snowpark
- Jeongseon Alpine Centre
- Alpensia Mountain Resort

Sources: Esri, HERE, DeLorme, USGS, Intermap, INCREMENT P, NRCan, Esri Japan, METI, Esri China (Hong Kong), Esri Korea, Esri (Thailand), MapmyIndia, NGCC, © OpenStreetMap contributors, and the GIS User Community.
Olympic Clusters Overview

- **PyeongChang Mountain Cluster** (Alpensia Mountain Resort)
- **Gangneung Coastal Cluster**

Sources: Esri, HERE, DeLorme, USGS, Intermap, INCREMENT P, NRCan, Esri Japan, Esri China (Hong Kong), Esri Korea, Esri (Thailand), MapmyIndia, NGCC, © OpenStreetMap contributors, and the GIS User Community