IFC Sustainability Webinar Series
June 1, 2017
Security Forces Handbook
Felicity Kolp
Social Development Specialist
IFC’s Security Forces Handbook

Now available at www.ifc.org/securityforces
IFC’s Security Forces Handbook

- Practical, project-level guidance
- Focused on PS4 implementation
- For IFC clients & other companies/consultants
- Downloadable tools

www.ifc.org/securityforces
WEBINAR AGENDA

• Intro to IFC and the Performance Standards

• Content of the handbook
  → Risk assessment
  → Private & public security, security mgmt plan, assessing allegations

• Potential uses of the handbook
  Questions
Intro to IFC and the Performance Standards
Global development institution providing & mobilizing capital & knowledge to the **private sector** operating in **developing countries**
• 2000+ clients
• Across regions
• Across sectors
• Reaching beyond clients
  \(\rightarrow\) international convergence on Environmental & Social (E&S) standards
IFC Performance Standards

→ IFC clients’ E&S responsibilities
  ▪ Strategic commitment to sustainable development
  ▪ Minimization & management of E&S risks & impacts

→ Globally recognized benchmark for E&S risk management in the private sector
  ▪ Apply to IFC’s investment and advisory projects
  ▪ May also be applied by other financial institutions
IFC Performance Standards

PS1: Assessment and Management of E&S Risks and Impacts

PS2: Labor and Working Conditions

PS3: Resource Efficiency and Pollution Prevention

PS4: Community Health, Safety and Security

PS5: Land Acquisition and Involuntary Resettlement

PS6: Biodiversity Conservation and Sustainable Management of Living Natural Resources

PS7: Indigenous Peoples

PS8: Cultural Heritage
Overview
Community Health and Safety
Emergency Preparedness
Security Personnel
PS4 Requirements

• **PS4 Para 12: Private Security**
  o Risk assessment
  o Hiring and employment
  o Conduct & use of force
  o Training
  o Grievance mechanism

• **PS4 Para 13: Public Security**
  o Risk assessment
  o Seek to ensure appropriate actions

• **PS4 Para 14: Allegations & Incidents**
  o Assess & address
PS4 Requirements in the Handbook

- **PS4 Para 12: Private Security**
  - Chapter 2 (risk assessment)
  - Chapter 3 (managing private security)
  - Chapter 5 (security management plan)

- **PS4 Para 13: Public Security**
  - Chapter 2 (risk assessment)
  - Chapter 4 (managing relationship w/public security)

- **PS4 Para 14: Allegations & incidents**
  - Chapter 6 (assessing allegations/incidents)
PS4 Requirements – Quick Reference

1. Assess Risks
   Assessing security risks can be simple and straightforward in low-risk contexts. The person responsible for security—ideally with input from other departments—should consider:
   - Security Risks (p. 23)
     - What might reasonably happen that would require some type of action by security (security guards, police, army)?
   - Security Response (pp. 24–25)
     - How are those security personnel likely to react and respond to those identified risks?
   - Potential Impacts (pp. 26–29)
     - What are the potential impacts from that response, focusing especially on impacts on communities?
   Document the outcomes of this process through a Risk-Response Chart (p. 30) or any other basic format (e.g., Excel sheet) that captures the potential risks, responses, and impacts.

2. Prevent and Mitigate Impacts
   As with other Performance Standards issues, companies should seek to avoid, minimize, and compensate for or offset negative impacts. Where potential risks or impacts are identified, companies should consider two key questions:
   - How can potential risks or impacts be prevented before they happen?
   - How can negative impacts be mitigated after they happen?
   Companies can prevent or mitigate negative impacts through corporate policies and engagement with private security (Chapter III) or public security (Chapter IV). These efforts should also be reflected in a Security Management Plan (Chapter V, pp. 81–87). In low-risk contexts, this plan may be relatively brief and may be incorporated into other policies and procedures as part of a company’s broader Environmental and Social Management System.

3. Manage Private Security
   Private security guards may be company employees or be contracted through a third-party security provider. Regardless, companies retain responsibility for ensuring that minimum standards are met—either through their own contracts and enforcement or through oversight of private security providers. This includes attention to:
   - Verting (pp. 46–47)
     - Who is providing security? Does anything in the guards’ background give cause for concern? Companies need to make reasonable inquiries to ensure that no guard has a history of past abuse or dishonesty. This may involve background checks or cross-checking with other companies, domestic or foreign government officials, UN missions, etc., as appropriate to the country context.
   - Ensuring appropriate use of force (pp. 46, 48)
     - Do guards know what is expected of them? Are they prepared to react with appropriate and proportional force in any situation? Companies should use their policies and procedures, reinforced by training, to provide clear instructions to directly employed guards. This can be as simple as including a clause in the employment contract setting out expectations, and following up with training.
   - Training (p. 49)
     - What will a guard do if a community member approaches in a nonthreatening way? In a threatening way? Training should focus on appropriate behavior and use of force. In low-risk contexts this can involve just a brief review of policies and procedures, recorded in a log, to ensure that guards understand how to respond to common interactions and scenarios.
   - Equipping (pp. 49, 51)
     - Do guards have what they need to do their jobs properly and safely? This usually means a uniform and identification and some type of communication device (typically a radio). In some cases it includes non-lethal weapons, such as pepper spray. The decision to arm guards with lethal force, such as a gun (pp. 51–52), is a serious one that should derive from the assessment of risk and be accompanied with a dedicated training program.
   - Monitoring (p. 53)
     - Are guards performing professionally and appropriately? Companies should check to confirm that policies and procedures remain relevant, and that guards are aware of and following them.
   Companies contracting security services still retain oversight responsibility of third-party security providers to ensure appropriate vetting, use of force, training, equipping, and monitoring of guards.

4. Manage the Relationship with Public Security
   Particularly in low-risk contexts, companies may have limited interactions with public security forces—this is especially true regarding national forces, such as the army or navy. Still, most companies are likely to need support from at least the local police in the case of an incident, and it’s important to understand who will be responding, and how. The focus is on assessment and engagement, building on key questions, such as:
   - Public Security Response (pp. 62–65)
     - When are public security forces likely to be involved? (e.g., only when called on, or potentially in other cases as well?) What type of individual or unit is likely to respond? How are they likely to respond? (e.g., what kind of capacity, mandate, reputation, etc., do they have, and how might this apply to likely scenarios involving the company?)
   - Engagement (pp. 66–74)
     - Are there opportunities to establish a relationship with police or other relevant public security forces? Companies are encouraged to reach out to authorities—preferably in advance of any issue—to understand potential deployments and, to the extent possible, to promote appropriate and proportional use of force. In low-risk contexts, this may involve simply making introductions to the local police commander and initiating a discussion about when and how authorities are likely to respond to incidents at the company or involving company personnel.
   - Documentation (p. 75)
     - Companies should document their engagement efforts, whether or not they are successful (e.g., in a basic meeting log with dates, attendees, and key topics).

5. Address Grievances
   When security problems arise or communities have complaints, companies should ensure that they have a method to respond. This generally involves:
   - Receiving Complaints (p. 94)
     - How can communities share information about allegations or incidents? (What is the company’s grievance mechanism?) How are complaints recorded and information collected?
   - Assessing (p. 95)
     - How are complaints considered? What type of inquiry is undertaken for more serious issues? (What is the company’s inquiry procedure?) Companies should record their information, analysis, and any conclusions or recommendations in a basic memo or incident report.
   - Reporting (p. 96)
     - Alleged illegal acts should be reported to the proper authorities.
   - Acting and Monitoring (pp. 95–96)
     - What can be done to prevent recurrence? Are remedial actions needed for affected parties? Companies are encouraged to identify lessons learned and to integrate these into future practices and, where appropriate, to communicate them to external stakeholders.
Content of the handbook
CHAPTER 2: RISK ASSESSMENT

Assess security risks to

- Identify, evaluate, and prioritize risks and likely security responses
- Understand and respond to community concerns and perceptions
- Determine appropriate security arrangements
- Inform mitigation plans and project resource implications
Risk assessment should be done as early as possible, but is a valuable tool at any stage of operations. It should be undertaken even if no assessment was done at project initiation.

“You can’t manage what you don’t know”
Project example:

- High-risk context, high-risk sector
- No previous PS4 assessment of security risks
- Complicated political situation → authorities threatening to take project “by force”
10 Questions All Companies Should Answer

1. What are the potential risks to the project that may require a security response?
2. How likely is it that these risks will occur?
3. What would be the likely security response?
4. If a security incident/response happens, what would be the impacts on the company?
5. How severe would these impacts be on the company?
6. If a security incident/response happens, what would be the impact on the community?
7. How severe would these impacts be on the community?
8. What are possible mitigation measures that prevent or reduce negative impacts?
9. Which risks are highest priority for mitigation, based on likelihood and severity of impact?
10. Is a full Security Risk Assessment needed?
# Security Risk Assessment

## Potential Risks to a Project That May Require a Security Response

<table>
<thead>
<tr>
<th>More Common Risks</th>
<th>More Serious Risks</th>
<th>Rare, Severe Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most projects have at least some risk of</td>
<td>Projects in more complex security</td>
<td>Few projects face such intense security risks, which typically are found only in</td>
</tr>
<tr>
<td>these occurring</td>
<td>environments may face these risks</td>
<td>more conflicted areas</td>
</tr>
<tr>
<td>Trespassing</td>
<td>Robbery</td>
<td></td>
</tr>
<tr>
<td>Vandalism</td>
<td>Assault</td>
<td></td>
</tr>
<tr>
<td>Petty theft</td>
<td>Armed protest</td>
<td></td>
</tr>
<tr>
<td>Roadblock</td>
<td>Sabotage of company property or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>operation</td>
<td></td>
</tr>
<tr>
<td>Community protests</td>
<td>Shooting or other use of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>offensive weapons</td>
<td></td>
</tr>
</tbody>
</table>

## Potential Responses by Security Personnel

### Passive Deterrents
- Access Control
  - Physical measures to prevent access to or passage through restricted areas, such as
    - Guards
    - Perimeter barriers
    - Surveillance systems

### Active Deterrents (Actions that are never acceptable are in purple italics)
- Verbal instructions, warning, refusal of passage/entry
- Guards issue verbal warnings to people who attempt or threaten to attempt to circumvent physical deterrents. These warnings may be followed by the use of physical deterrents if the threat is being continued.

### Escalation (Actions that are never acceptable are in purple italics)
- Use of nonlethal force
  - Guards use nonlethal force defensively (e.g., batons, nonlethal ammunition) to repel an external physical threat, subject to existing use-of-force protocols.
- Arrest by public authorities
  - Guards request the intervention of police to apprehend and/or arrest people alleged to have committed criminal acts such as theft, trespass, assault.
### Sample SRA & Heat Map

<table>
<thead>
<tr>
<th>STEPS</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk</td>
<td>Likelihood</td>
<td>Security Response</td>
<td>Impact on Company</td>
<td>Severity</td>
<td>Impact on Community</td>
<td>Severity</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td>4</td>
<td>Access controls to prevent theft; private security guards may apprehend suspected thieves and turn them over to authorities</td>
<td>Loss of company property; potential danger to employees if thieves take property by force</td>
<td>2</td>
<td>Alleged thieves risk injury or mistreatment during apprehension and/or detention</td>
<td>3</td>
<td>Ensure that guards have clear guidelines for apprehension and short-term detention; encourage police to treat suspects appropriately</td>
<td></td>
</tr>
<tr>
<td>Protest</td>
<td>3</td>
<td>Prevent or control access to site; public security may respond physically if protest becomes violent</td>
<td>Disruption to operations, particularly staff access to site and transportation; possible injury to employees</td>
<td>4</td>
<td>Injuries sustained from any use of force (justified or otherwise) against a protest; community resentment toward company</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trespass</td>
<td>2</td>
<td>Access controls to prevent access, including clear signage; guards may confront people attempting to walk through site</td>
<td>Potential safety hazard and disruption to operations</td>
<td>2</td>
<td>Frustration among community that pre-existing access/transit routes are no longer available; injuries sustained by community members entering hazardous areas of the site</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harassment of women by security guards</td>
<td>3</td>
<td>Presence of security forces generates potential threat</td>
<td>Limited immediate impact; potential secondary impact to operations and/or reputation from community reaction</td>
<td>1</td>
<td>Verbal harassment and/or physical violation of community members, particularly women</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Heat Map
- **High Impact**
- **Low Impact**
- **Unlikely**
- **Near Certain**

- **Protest**
- **Theft**
- **Trespass**
- **Harassment**
**COMPANY EXAMPLE OF SRA**

<table>
<thead>
<tr>
<th>Security Risk to the Project</th>
<th>Likelihood of Risk Occurring (L/M/H)</th>
<th>Severity of Impact on Company (L/M/H)</th>
<th>Security Responder (Public/Private)</th>
<th>Expected Response</th>
<th>Impact Expected Response on Community</th>
<th>Severity of Impact on Community (L/M/H)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community gathering someone and holds hostage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extortion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threats to the workforce</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assaults on personnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project taken by the outside forces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental problems leading to security issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labor strikes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workers' rights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Robbery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**THREAT REGISTER**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Threat</th>
<th>Risk</th>
<th>Probability/Likelihood</th>
<th>Impact</th>
<th>P x I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Loss of property, theft, or damage to property</td>
<td>High</td>
<td>8</td>
<td>Low</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Construction of a new business</td>
<td>Medium</td>
<td>5</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Natural disaster, flood, fire, etc.</td>
<td>Medium</td>
<td>5</td>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Insufficient security at the site</td>
<td>Medium</td>
<td>5</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Inadequate training of security guards</td>
<td>Low</td>
<td>1</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Insufficient access control</td>
<td>Medium</td>
<td>5</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>Inadequate management of project security</td>
<td>Low</td>
<td>1</td>
<td>Low</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>Insufficient monitoring of site</td>
<td>Medium</td>
<td>5</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>Insufficient enforcement of security policies</td>
<td>Low</td>
<td>1</td>
<td>Medium</td>
<td>3</td>
</tr>
</tbody>
</table>
COMPANY EXAMPLE OF SRA

Risk Assessment (Before Mitigation)

Risk Assessment (AFTER Mitigation)

Security Risk matrix

RISK MANAGEMENT MITIGATION
Chapter 3: Private Security

Private Security should be:

- Contracted with the goal of providing physical protection and risk reduction
- Typically under company control and governed by contract provisions
- Properly vetted, trained, equipped, and monitored
- Unarmed unless shown to be necessary and appropriate by the risk analysis
**PRIVATE SECURITY**

Private security ➔ within company’s control

**Areas to Consider:**

<table>
<thead>
<tr>
<th>Private Security</th>
<th>Oversight</th>
<th>Contract</th>
<th>Vetting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Retain control over and responsibility for employees’ behavior and quality</td>
<td>Include performance standards and monitoring provisions</td>
<td>Check backgrounds and avoid hiring anyone with history of abuse</td>
</tr>
<tr>
<td><strong>Conduct</strong></td>
<td>Require appropriate behavior through policies and procedures, reinforced through training</td>
<td>Ensure force is used only for preventive and defensive purposes and in proportion to the threat</td>
<td>Train guards on use of force, appropriate conduct, and firearms</td>
</tr>
<tr>
<td><strong>Equipment</strong></td>
<td><strong>Weapons</strong></td>
<td><strong>Incidents</strong></td>
<td><strong>Monitoring</strong></td>
</tr>
<tr>
<td>Provide guards with identification, communications device, and any other necessary equipment for the job</td>
<td>Equip guards with non-lethal force and arm them only when justified by SRA</td>
<td>Ensure ability to receive and assess incident reports and other complaints</td>
<td>Ensure appropriate conduct through document review, audits, training, and evaluation of incident reports or complaints</td>
</tr>
</tbody>
</table>
PRIVATE SECURITY

Private security → within company’s control

• Contract is key
  o Background checks & hiring
  o Expectations for conduct & use of force
  o Grievance mechanism
  o Training
  o Supervision

A company can outsource its security, but it cannot outsource its responsibility.
CHAPTER 4: PUBLIC SECURITY

Focus on engagement, recognizing that public security forces report through a hierarchy external to the company.

Assess and document risks arising from the use of public security forces.

To the extent possible, seek to influence public security to conform with good practice.

Company efforts regarding public security forces should...
Public security ➔ reporting line outside company

• Risk assessment

Figure 16: Security Risk Spectrum and Public Security Involvement

- Low-Level Risk:
  - On-call law enforcement from off-site
  - General law enforcement
  - Security for hazardous materials
  - Convoy security

- Moderate-Level Risk:
  - Nearby off-site or on-site security backup
  - Immediately available to handle protests or civil disturbance
  - Armed convoy security
  - Close personal protection

- High-Level Risk:
  - Dedicated and heavy on-site security as protection from armed groups
  - Perimeter security
  - Defensive patrols outside the perimeter
Public Security

Public security → reporting line outside company

- Risk assessment
- Engagement efforts (and documentation of efforts)

Box 10: Using Active Engagement with Government Authorities to Manage Security Risks and Avoid Escalation

Box 11: Small Acts of Disrespect Can Escalate into Serious Security Situations

Box 12: Risks Related to Equipment Transfers

Box 13: Reducing Risks Related to Public Security Forces

Even though companies are not directly responsible for the actions of public security forces, they may be linked to their behavior in the eyes of community...
## Public Security

### Topics for Engagement with Public Security Forces

<table>
<thead>
<tr>
<th>1</th>
<th>What are the types of public security forces involved?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>What is the number and role of public security personnel involved?</td>
</tr>
<tr>
<td>3</td>
<td>What type of public security response is likely to be used?</td>
</tr>
<tr>
<td>4</td>
<td>What is the background and track record of these public security forces?</td>
</tr>
<tr>
<td>5</td>
<td>How should risks be documented?</td>
</tr>
</tbody>
</table>

### 5 Questions to Address Public Security Risks

<table>
<thead>
<tr>
<th>Engagement</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal introductions, willingness to engage, identification of appropriate representatives, establishment of regular meetings</td>
<td>Type and number of guards and the competency, appropriateness, and proportionality of this deployment</td>
</tr>
</tbody>
</table>

### Community Relations

Potential impacts on communities, and any engagement efforts, including grievance mechanism and any known complaints

### Use of Force

Security force deployment and conduct, including desire for preventive and proportional responses

### Security Personnel

Background and reputation of security personnel, to the extent possible, and engagement and monitoring efforts

### Training

Current provision of any training and opportunities to collaborate on capacity building, as appropriate

### Equipment

Existing needs and potential offers, expectations, and conditionalities, including implementation of restrictions, controls, and monitoring

### Incidents

Policies and procedures for recording, reporting, and monitoring allegations of unlawful or abusive acts
Public Security

Public security → reporting line outside company

- Relationship is key
  - Engagement
  - Deployment
  - Training
  - Equipment
  - Use of Force
CHAPTER 5: SECURITY MANAGEMENT PLAN

Security Management Plans should

- Describe security functions, responsibilities, required resources, management, and delivery
- Respond to identified risks, with SMP size and scope based on the Security Risk Assessment
- Include all relevant policies and procedures guiding security provision
- Mitigation measures should address risks and impacts on communities as well as on company
Elements of an SMP

- Overview of Security Situation
- Physical Security
- Security Operating Procedures
- Security Supervision and Control
- Private Security Force Management
- Managing Relations with Public Security
- Incident Reporting and Inquiry
- Community Engagement and Grievance Mechanism
- Objectives, Mission, and Approach of Company Security
- Company Policies and Standards Relevant to Security

Security Management Plan
SECURITY MANAGEMENT PLAN

• Mitigation measures correspond to identified risks
  → To company
  → To community and employees

• SMP as part of E&S Management System
  → Stand-alone or integrated into broader mgmt plans
Chapter 6: Assessing Allegations

In Assessing Security-Related Allegations or Incidents

Scope and effort should be commensurate with severity and credibility of allegation or incident

Companies should establish policies and procedures for receiving, assessing, and documenting security-related allegations or incidents

Key aspects include documentation, information collection, confidentiality protection, inquiry and assessment, reporting, corrective action, and monitoring and communicating

Unlawful or abusive acts should be reported to authorities
Key Steps in Assessing Security-Related Allegations or Incidents

- Record the incident or allegation
- Collect information promptly
- Protect confidentiality
- Assess the allegation or incident

- Monitor and communicate outcomes
- Take corrective action to avoid recurrence
- Report any unlawful act
- Document the process
- Conduct further inquiry, if warranted
ASSESSING ALLEGATIONS OR INCIDENTS

Lessons learned:

• Difficult to reconstruct circumstances long after an incident

• Establish basic protocols in advance
  o Record and document
  o Assess and inquire
  o Monitor and communicate

• Community engagement is key

• Take corrective action to avoid recurrence
TOOLS AND TEMPLATES

• PDF in Handbook + Word doc downloads

• Additional guidance

• Ready-to-use templates

“insert logo here”

COMPANY LOGO

• Drafting an SMP
• Further Resources

RFP for SRA/SMP
Contract w/ Private Security Provider
Incident Report
MoU
Potential uses of the handbook
Annex C. Template Contract with a Private Security

How to Use?

- Read cover to cover
- Reference relevant chapter(s)
- Use templates as needed
- Focus on the graphics to ensure the basics
- Focus on risk assessment
- Review recommendations for lower-risk contexts

Key Takeaway for Lower-Risk Contexts

IFC - International Finance Corporation
WORLD BANK GROUP
THANK YOU!

“I want to know any issues or concerns that our communities have. If they don’t get solved proactively, they can end up at the gate. And that is often too late.”

—Security Manager at a large, high-risk site

www.ifc.org/securityforces

asksustainability@ifc.org