SAFER SOCIETY

2025

Transparency Report

Contents

1 Chairman's Note: A New Phase of Accountability

The year 2025 marks a significant transition for NSO Group. With new ownership based in the United States and my appointment as Executive Chairman, the Company is entering a new phase defined by strengthened governance, clearer strategic direction, and a renewed focus on accountability in an increasingly complex global environment. NSO embarks on this path while maintaining and advancing its unique technologies, in order to provide its governmental clients with best-in-class products to serve their legitimate and necessary law enforcement and national security functions.

Having spent much of my professional career working at the intersection of law, public policy, and regulated industries, I am acutely aware that technologies with significant public-interest implications demand more than technical excellence. They require disciplined governance, credible oversight, and sustained engagement with regulators, policymakers, and society. NSO operates in one of the most sensitive areas of the technology sector. Our products support government authorities confronting serious threats such as terrorism and organized crime, while also carrying real risks to fundamental rights if misused. Managing this tension responsibly is foundational to the Company's legitimacy and long-term sustainability.

To put it simply, when NSO's products are in the right hands within the right countries, the world is a far safer place. That will always be our overriding mission.

Over recent years, NSO has invested significantly in building and operationalizing a robust human rights and compliance framework. Well before international initiatives gained momentum in this area, the Company adopted a Human Rights Policy aligned with the UN Guiding Principles on Business and Human Rights, established dedicated governance and compliance structures, and committed to publishing detailed Transparency & Responsibility Reports. These efforts reflect a clear understanding that responsible conduct in this sector cannot be reactive or purely procedural; it must be embedded in decision-making, product design, customer engagement and corporate culture.

It is equally clear that no single Company – regardless of the maturity of its internal controls – can address the challenges posed by a global and fragmented cyber intelligence market on its own. The emergence of multilateral and multistakeholder initiatives, including the Pall Mall Process initiated by the United Kingdom and France, in which the United States now participates, reflects growing international consensus on the need for coordination. The principles articulated through that process – accountability, precision, oversight, and transparency – closely align with safeguards NSO has already implemented and signal a broader shift toward shared responsibility across governments, industry, civil society, and the research community.

As Executive Chairman, my responsibility is to ensure that NSO continues to lead by example – by delivering outstanding and life-saving results to its customers while maintaining rigorous internal safeguards, and by engaging constructively in the development of external frameworks that can raise standards across the sector. This includes supporting clearer definitions of legitimate use, advocating for coherent licensing and oversight mechanisms, and contributing to dialogue grounded in realism about both security needs and human rights protections.

This report reflects that commitment. It sets out where NSO stands today, how our governance and compliance structures have evolved, and where we believe the sector should go next. Accountability in this domain is not a destination but an ongoing process. Our objective is to ensure that NSO remains a responsible and highly effective actor – one

that earns trust through action and recognizes that transparency and oversight are essential to sustaining both security and human rights.

Thank you for your interest in NSO Group.

Sincerely,

David Friedman

Executive Chairman

2 About NSO Group

2.1 Ownership, Governance, and Leadership

In 2025, NSO Group entered a new phase of its corporate development following a change in ownership and the appointment of David Friedman as the new Executive Chairman of its holding Company. This transition is part of the ongoing effort to strengthen the Company's governance framework, reinforce independent oversight, and support the long-term sustainability of NSO's compliance-driven operating model. The new ownership structure brings a continued focus on transparency, risk management, and alignment with evolving international expectations regarding the responsible development and deployment of sensitive technologies.

As part of this transition, NSO refreshed its Board-level governance architecture, including the composition and mandate of the Governance, Risk and Compliance Committee (GRCC). The GRCC plays a central role in overseeing ethical standards, the human rights compliance program, and the Company's risk appetite. It serves as a key control point for reviewing and approving business engagements identified as presenting elevated legal, ethical, or human rights risk.

2.2 Mission and Operational Scope

NSO Group's mission is to support legitimate government authorities in addressing serious threats to public safety, including terrorism and organized crime, through the provision of narrowly scoped, targeted cyber intelligence technologies. Criminal and terrorist actors increasingly exploit encrypted communications and digital anonymity to evade detection, creating significant challenges for law enforcement and intelligence agencies operating under the rule of law. NSO's technologies are designed to assist lawful, targeted investigations where other investigative tools may be insufficient.

2.3 Regulatory Status and Export Controls

NSO Group's products are classified as "defense articles" under Israeli law and are subject to one of the most stringent export control regimes applicable to cyber technologies. Every marketing activity and export transaction requires prior authorization from the Israeli Ministry of Defense through the Defense Exports Control Agency (DECA). This licensing process includes a review of the proposed customer, the intended use of the technology, and broader national security and human rights considerations.

Export licenses are issued on a transaction-specific basis and are subject to renewal and ongoing governmental oversight. As part of the export licensing process, customer governments are required to execute an End-User Certificate (EUC), which formally identifies the authorized end-user, specifies the permitted purpose of use, and includes binding commitments regarding non-transfer, non-diversion, and compliance with applicable legal and regulatory requirements. These external regulatory requirements operate alongside NSO's internal compliance controls and constitute a critical layer of independent supervision over the Company's activities.

2.4 Products and Built-In Safeguards

NSO develops a limited number of cyber intelligence products designed for targeted use against specific, pre-identified threats. These products are not mass-surveillance tools and are designed to operate within defined technical and legal boundaries. Safeguards are embedded at multiple levels, including restrictions on scope, duration, geography, and the number of permitted targets, as well as mechanisms intended to prevent unauthorized transfer or modification.

While the details of technical features of NSO's products are not public due to obvious legal and confidentiality constraints, the Company has publicly described in prior Transparency & Responsibility Reports a range of safeguards designed to mitigate misuse risks. These include system-level controls, audit and logging capabilities, and the ability to suspend or disable systems in response to credible indications of misuse. The development and refinement of such safeguards is an ongoing process, informed by lessons learned, technological advances, and evolving best practices.

2.5 Risk Management and Oversight Framework

NSO's operating model is supported by an integrated risk management framework that combines Board-level oversight, executive accountability, and a dedicated compliance function. The Compliance Team works closely with legal, technical, and business units to ensure that risk considerations – including human rights risks – are identified early and addressed throughout the lifecycle of customer engagements.

The Governance, Risk and Compliance Committee serves as a key escalation and decision-making body for matters involving heightened risk, while senior management remains responsible for ensuring that approved mitigation measures are implemented and monitored. This multilayered approach reflects NSO's recognition that effective governance in the cyber intelligence domain requires both structural controls and a strong organizational culture of responsibility.

3 Our Commitment to Human Rights

3.1 NSO's Human Rights Philosophy

NSO Group's approach to human rights reflects the reality that cyber intelligence technologies operate at the intersection of public safety, national security, and fundamental freedoms. Such capabilities can play a legitimate and vital role in protecting societies from terrorism, organized crime, and other serious threats, while misuse can result in serious harm to individual rights. NSO's human rights philosophy is therefore grounded in a dual obligation: to support lawful government efforts to protect public safety and to exercise responsibility within the Company's sphere of influence to prevent, mitigate, and respond to misuse.

NSO rejects simplistic narratives that treat cyber intelligence technology as either inherently abusive or inherently necessary. Instead, NSO treats human rights as a matter of governance, risk management, and institutional design, recognizing that responsibility depends not only on legal compliance, but on anticipating risk, embedding safeguards into products and processes, and enforcing clear standards of conduct across the lifecycle of customer engagements.

3.2 Alignment with International Human Rights Standards

NSO Group's human rights framework is explicitly aligned with the United Nations Guiding Principles on Business and Human Rights (UNGPs), Since adopting its Human Rights Policy in 2019, NSO has worked to operationalize the UNGPs across governance, due diligence, contractual arrangements, trainings, investigations, and remediation. This approach is further informed by relevant international standards, including the OECD Guidelines for Multinational Enterprises, and relevant guidance issued by the U.S. Department of State on transactions linked to foreign government end-users of surveillance technologies, and applicable international human rights law.

Operational alignment is reflected in NSO's human rights compliance program, which integrates due diligence throughout the product lifecycle – from research and development, through customer evaluation and licensing, to post-sale monitoring and investigation of allegations. Policies and procedures are reviewed periodically to ensure they remain responsive to legal developments, technological change, and lessons learned.

3.3 The Investigative Context: Necessity and the "Going Dark" Challenge

The regulation of cyber intelligence technologies must be understood in light of the investigative realities that led to their development. Over more than a decade, law enforcement and security agencies have faced a structural shift in the communications environment. The widespread adoption of end-to-end encryption, anonymization services, and reduced data retention has significantly limited the effectiveness of traditional lawful interception tools.

The "going dark" challenge reflects changes in how serious criminal and terrorist activity is organized and concealed. In many cases, conventional investigative methods are ineffective even where legal thresholds for their use have been met. Cyber intelligence

technologies were developed as a targeted response to this gap, enabling lawful authorities, acting under applicable legal frameworks, to obtain access to information necessary to investigate and prevent the most serious threats to public safety when other means are insufficient.

This necessity is recognized in international law. Article 20 of the United Nations Convention against Transnational Organized Crime (UNTOC) expressly acknowledges the use of "special investigative techniques", including modern electronic methods, subject to domestic law, safeguards and oversight. Such tools are intended as exceptional tools, typically reserved for cases involving serious crime or terrorism, and governed by legal authorization, purpose limitation, and independent supervision.

Understanding this necessity is essential to any balanced assessment of cyber intelligence technologies. Regulation cannot be grounded solely in the risks of misuse. It must also take account of the legitimate public interest in protecting lives, dismantling criminal networks, and preventing grave harm. The challenge for policymakers, regulators, and industry is therefore not whether such capabilities should exist in principle, but how they can be governed, constrained, and overseen in a manner consistent with the rule of law and respect for human rights. In this regard, NSO stands as the industry leader in terms of both the effectiveness of its products and the seriousness it attaches to the proper use of those products.

3.4 Human Rights Risks in the Cyber Intelligence Context

NSO recognizes that cyber intelligence technologies present distinct human rights risks arising from their potential intrusiveness, the sensitivity of the information involved, and the imbalance of power between state authorities and targeted individuals. If misused, such technologies can infringe on the right to privacy, freedom of expression and association, and due process, particularly in environments with weak legal frameworks or insufficient oversight.

At the same time, the use of cyber intelligence technologies engages other protected interests, including the rights to life, security, and effective protection from serious crime and violence. International human rights law recognizes that privacy or expression rights are not absolute and may be subject to lawful, necessary, and proportionate limitations in pursuit of legitimate aims such as public safety and crime prevention.

Certain groups – including journalists, human rights defenders, lawyers, political activists, and civil society actors – face elevated risks and therefore require heightened scrutiny, and strong institutional safeguards governing any deployment of cyber intelligence capabilities.

3.5 How Risk Recognition Informs NSO's Decisions

Recognition of these risks directly informs NSO's operational decisions. Human rights risk assessment is central to NSO's customer vetting and due diligence processes. Prior to any engagement, NSO evaluates the political and legal environment of the prospective customer, including surveillance laws, judicial independence, and oversight mechanisms.

Where risks cannot be adequately mitigated, NSO does not proceed with the engagement. Where mitigation is possible, NSO applies layered safeguards calibrated to the risk profile, including contractual restrictions, technical limitations, enhanced training, and post-sale monitoring. NSO also monitors relevant developments over time and initiates internal review and investigations where credible allegations may arise.

3.6 Preventing Proliferation and Misuse

NSO recognizes that cyber intelligence capabilities are powerful tools whose misuse can cause serious harm to human rights, national security, and international stability. The central risk in this domain is not only misuse by authorized actors, but proliferation to the wrong actors. Preventing NSO's technology from falling into the hands of hostile states, terrorist organizations, transnational criminal networks, or other actors operating outside the rule of law is therefore a foundational element of the Company's approach to responsible governance.

NSO's compliance philosophy is built on the premise that non-proliferation is itself a security safeguard. Technologies that never reach malicious or irresponsible actors cannot be used to repress populations, undermine democratic institutions, or destabilize international security. For this reason, NSO treats cyber intelligence technologies as belonging to a category of sensitive capabilities that require special controls and non-proliferation regimes, similar in logic to those applied to other strategic or dual-use technologies. This principle has guided the design of NSO's compliance program from its inception.

To operationalize this philosophy, NSO's compliance framework is structured around multiple, mutually reinforcing defense layers. These include state-level export controls, the Company's own due diligence, post-sale enforcement and termination mechanisms. Each of these layers is described in detail in this report. Together, they are intended to ensure that NSO's technology is transferred only to authorized end-users, used for legitimate purposes, and withdrawn where conditions of use are violated.

Non-proliferation is also embedded directly into NSO's technical design choices. NSO's products are delivered as closed, "black-box" systems. Customers do not receive access to underlying source code, exploit components, or individual vulnerabilities and cannot extract, modify, or repurpose the technology independently. The systems are bound to specific hardware, network environments and configurations approved at the time of licensing, and they are designed to be inoperable outside those authorized parameters.

Access to vulnerabilities and other sensitive technical components within NSO is tightly controlled through internal compartmentalization and strict access restrictions. Vulnerabilities are never transferred directly to customers. Instead, they are embedded in encrypted form within NSO's products. This architecture is intended to prevent unauthorized transfer, reverse engineering, or independent reuse, even by authorized customers.

These design and governance choices reflect NSO's view that preventing proliferation is closely linked to responsible use. By limiting access, restricting transfer, and building technical and organizational controls into its systems, NSO seeks to reduce the risk that its technology could be obtained or misused by actors operating outside lawful and accountable frameworks. This approach aligns with broader international efforts to manage the risks associated with sensitive technologies while supporting legitimate security needs.

3.7 The Unique Structural Architecture of Compliance in the Cyber Intelligence Domain

NSO Group is transparent about the structural parameters within which its compliance framework operates – and views these parameters as a core strength of responsible

governance in the cyber intelligence sector. As a private technology provider, NSO does not operate its products, does not select targets, and does not access operational data. Decisions regarding the deployment of cyber intelligence capabilities are taken exclusively by sovereign government authorities, acting pursuant to their own legal mandates, authorization requirements, and accountability mechanisms.

This separation between provider and end-user is not a shortcoming. It is a defining and intentional feature of the industry's governance architecture. It ensures that sensitive operational information, including data relating to investigative targets, remains exclusively within the hands of authorities that are legally empowered to access it, and is not disclosed to or controlled by private actors. Operational decisions therefore remain subject to state authority, judicial oversight, and domestic legal safeguards, rather than being exercised by private actors. Within this model, NSO's responsibility is clearly delineated and rigorously executed: to conduct robust pre-sale human rights due diligence, impose enforceable contractual restrictions, embed technical safeguards, monitor risk indicators, and respond decisively where credible concerns arise.

By maintaining this clear division of roles, NSO avoids assuming functions that properly belong to states, courts, and oversight bodies, while maximizing accountability within its own sphere of influence. Effective protection of human rights in the cyber intelligence domain depends not on the concentration of control in private hands, but on the proper functioning of domestic legal systems, independent oversight institutions, and coordinated international frameworks. NSO's compliance program is designed precisely to operate within – and reinforce – this ecosystem.

4 Human Rights Compliance Program

NSO Group has established and continuously refined a comprehensive human rights compliance program designed to identify, assess, prevent, mitigate, and respond to risks associated with the misuse of cyber intelligence technologies. The program reflects the specific risk profile of the cyber intelligence sector, where advanced investigative capabilities intersect with heightened human rights sensitivities and inherent structural constraints on provider oversight.

4.1 Governance and Oversight

Oversight of NSO Group's human rights compliance program is anchored at the highest levels of the organization. The Board of Directors retains ultimate responsibility for ethical direction, risk appetite, and compliance posture, supported on its behalf by the Governance, Risk and Compliance Committee (GRCC). The GRCC provides focused oversight of elevated legal, ethical, and human rights risks and serves as the primary escalation and decision-making forum for complex or high-risk engagements.

Day-to-day implementation is led by senior management and executed by a dedicated Compliance Team with expertise in human rights due diligence, investigations, and regulatory compliance. The Compliance Team operates independently from commercial functions and works closely with legal, technical, and operational teams to embed human rights considerations across customer onboarding, contractual arrangements, training, and post-sale oversight.

In parallel, NSO's most sensitive products are subject to independent external oversight through national export control authorities. As a regulated defense technology provider, all marketing and export activities require transaction-specific authorization from the Israeli Ministry of Defense through the Defense Exports Control Agency (DECA). Export licenses are time limited, subject to renewal, and granted following government review of the customer, intended use, and relevant national security and human rights considerations.

4.2 Human Rights Due Diligence

Human rights due diligence (HRDD) applies to all prospective and existing customer relationships. Its purpose is to assess the risk of misuse and determine whether identified risks can be adequately mitigated.

The process begins with a country-level assessment examining governance indicators such as respect for human rights, rule of law, judicial independence and corruption. Jurisdictions subject to credible international sanctions or embargoes are excluded as a matter of policy. NSO also evaluates the specific end-user organization, including its legal mandate, oversight structures, and the domestic legal framework governing surveillance activities.

Each engagement is assigned a risk classification. Low- and moderate-risk engagements may proceed subject to standard safeguards. Higher-risk engagements are subject to enhanced mitigation measures, including additional contractual restrictions, tailored technical limitations, training requirements, and closer post-sale monitoring. Where risks cannot be adequately mitigated, NSO does not proceed with the engagement.

HRDD is ongoing. Customer relationships are reassessed periodically, including through annual reviews, and may be reexamined in response to material changes in country conditions or credible external reporting.

4.3 Contractual and Technical Safeguards

NSO reinforces governance and due diligence through contractual and technical safeguards designed to restrict use of its technologies to legitimate purposes.

Customer agreements impose strict limitations, including limiting use solely for the prevention and investigation of terrorism and serious crime, compliance with applicable law, prohibitions on onward transfer, and requirements for lawful authorization prior to deployment. Customers must notify NSO of suspected misuse and cooperate with internal review processes.

Technical safeguards are embedded directly into NSO's products. These include limits on targets, geography, and duration of use. Systems are designed as targeted tools rather than mass-surveillance platforms. Deployment requires operator statements confirming lawful authorization, and system activity is recorded through immutable audit logs retained within the customer's environment. NSO does not have routine access to operational data or audit logs and may review them only with customer consent in the context of a defined compliance or misuse investigation. NSO also maintains the capability to suspend or disable systems where credible concerns of misuse arise.

4.4 Reporting, Investigations, and Remedies

NSO maintains internal and external whistleblowing mechanisms that allow employees, partners, customers, and affected third parties to raise concerns confidentially and, where necessary, anonymously. Whistleblowing policies and reporting instructions are publicly available on NSO's website and prohibit retaliation while requiring impartial handling of all reports.

Reports of suspected misuse are subject to an initial assessment by the Compliance Team. Where warranted, formal investigations are conducted in accordance with NSO's Potential Product Misuse Investigation Procedure and may involve customer engagement, review of legal frameworks, examination of audit logs (subject to constraints), and consultation with internal or external experts. Findings are escalated to senior management and, where appropriate, to the GRCC.

Depending on the outcome, NSO may require corrective actions, impose additional safeguards, suspend service, or terminate the customer relationship, including disabling the system where necessary.

NSO does not seek to replace state-based accountability or judicial remedies but supports the availability of grievance and remedy mechanisms at the customer and international levels as a complement to corporate compliance.

5 Human Rights in Our Value Chain

NSO Group recognizes that respect for human rights extends beyond its direct operations and includes the conduct of entities within its value chain. While NSO's business model differs from that of many commercial technology companies – given that it operates as a downstream provider of regulated defense technology to sovereign government

customers – the Company maintains a structured, risk-based approach to managing human rights and integrity risks associated with suppliers, service providers, and business partners.

The cyber intelligence sector presents distinct value-chain challenges. Supply relationships often involve highly specialized technical services, sensitive research functions, and long-term partnerships operating under strict confidentiality constraints. These characteristics require a tailored governance model that balances oversight and accountability with operational security and legal obligations.

5.1 Supplier Code of Conduct

NSO has adopted a Supplier Code of Conduct that establishes baseline expectations for ethical conduct, legal compliance, and respect for human rights across its supplier relationships. The Code applies to all suppliers, contractors, and service providers, is incorporated into procurement processes and contractual arrangements, and is publicly available on the Company's website.

The Code sets clear requirements relating to:

- Compliance with applicable laws
- Respect for internationally recognized human rights
- Prohibition of bribery, corruption, forced labor, child labor, and human trafficking
- Adherence to sanctions and export-control regimes
- Protection of confidential information
- Responsible labor and environmental practices

Material noncompliance may result in corrective action or termination of the relationship.

5.2 Supplier Due Diligence and Risk Assessment

Supplier due diligence is risk-based and proportionate to the nature of the goods or services provided. Standard assessments include verification of corporate identity and ownership, reputational and integrity screening, sanctions checks and review of anti-bribery and corruption controls.

Where suppliers are involved in particularly sensitive functions – such as technical research, vulnerability-related services, or access to proprietary systems – NSO applies enhanced due diligence measures. These include additional background checks, assessment of internal security controls, and strict confidentiality and non-disclosure obligations. Supplier relationships are subject to ongoing monitoring, and reassessment may be triggered by changes in ownership, geographic footprint, risk profile or credible external reporting.

5.3 Managing High-Sensitivity Supply Relationships

Certain aspects of NSO's value chain involve activities of heightened sensitivity. These relationships are managed through narrowly defined scopes of work, contractual safeguards, compartmentalization of sensitive functions, and technical and organizational access controls. Suppliers do not receive unrestricted access to NSO technologies,

codebases or operational systems and are bound by strict limitations on use and disclosure.

This approach prioritizes security, traceability, and accountability, while recognizing that full public transparency is neither feasible nor responsible in all circumstances.

5.4 Oversight, Enforcement, and Remediation

NSO retains the right to assess and, where appropriate, audit supplier compliance with contractual obligations and the Supplier Code of Conduct, subject to legal and operational constraints. Where potential violations are identified, NSO may engage with the supplier to seek clarification, require corrective actions, or impose additional safeguards. In cases of serious or repeated noncompliance, NSO may suspend or terminate the relationship.

Suppliers are expected to cooperate with NSO investigations where concerns arise, including those related to human rights, corruption, or misuse of sensitive information. Supplier-related risks are subject to the same internal escalation mechanisms as customer-related risks and may be reviewed by senior management or the Governance, Risk, and Compliance Committee where warranted.

5.5 Structural Considerations and Limits of Influence

NSO acknowledges that its influence over the value chain has defined limits. As a downstream provider licensing technology directly to sovereign government customers, NSO does not operate a broad or consumer-facing supply ecosystem. In addition, certain upstream markets – particularly those involving advanced technical research – are characterized by a limited number of qualified participants and heightened confidentiality requirements.

Within these parameters, NSO seeks to exercise leverage responsibly and proportionately. The Company's value-chain approach focuses on areas where it can reasonably influence conduct, enforce standards, and mitigate risk, while recognizing that broader human rights outcomes in the cyber intelligence domain ultimately depend on coordinated action by governments, regulators, and industry participants.

6 Stakeholder Engagement & NSO's Role in the Pall Mall Process

NSO Group operates in a domain where the consequences of misuse are significant, expectations for oversight are rising, and public trust depends on more than internal controls alone. For this reason, NSO approaches stakeholder engagement as a core element of responsible governance rather than as a communications exercise. Engagement informs how the Company identifies emerging risks, refines safeguards, evaluates legal and institutional environments and contributes to the development of coherent international norms governing commercial cyber intrusion capabilities (CCICs).

The Pall Mall Process reflects a broader shift toward international coordination in this space. Launched to address the proliferation and irresponsible use of CCICs, it brings together states, international organizations, industry, academia, and civil society to develop guiding principles across the CCIC lifecycle. The Pall Mall Summary Report highlights recurring concerns raised by participants, including the absence of shared definitions, unbalanced market incentives, and fragmented regulatory approaches in a rapidly evolving technological environment.

NSO's engagement in this process is grounded in operational experience. As a regulated defense technology provider operating under stringent export licensing requirements, with an established human rights compliance program and a record of implementing safeguards, investigations, and enforcement actions, NSO contributes a practical, implementation-focused perspective. This chapter outlines how NSO situates itself within the broader stakeholder ecosystem, summarizes its contributions to the Pall Mall Process, and identifies the structural gaps that remain in global governance frameworks.

6.1 How NSO Engages Across the Ecosystem

NSO's stakeholder engagement spans 5 principal communities, each contributing a distinct and necessary perspective on the responsible governance of CCICs.

1. **Governments and regulators** are engaged primarily through export-control licensing, compliance oversight, and dialogue on lawful, rights-respecting use of cyber intelligence technologies. NSO's operating model is shaped by transaction-specific licensing and ongoing regulatory supervision, providing insight into how legal frameworks function in practice and where greater cross-jurisdictional coordination is required.
2. **Civil society and human rights organizations** contribute information on real-world allegations, evolving risk patterns, and the impact of misuse on vulnerable groups, including journalists, activists, dissidents, and human rights defenders. NSO's compliance framework is designed to receive and assess credible external information, including civil-society reporting, as part of investigation intake and ongoing risk reassessment, subject to legal and confidentiality constraints.
3. **Academic and policy research communities** play an important role in advancing understanding of governance challenges associated with cyber intelligence capabilities. NSO's engagement in this area is deliberately bounded: The Company considers credible, publicly available research relevant to risk assessment and policy discussions, but does not engage in operational collaboration or information sharing that could compromise investigations, proprietary technology, or legal obligations.

4. **Industry peers** operate in a global and fragmented market characterized by divergent regulatory regimes. The Pall Mall Summary Report notes the absence of shared definitions and baseline expectations across the sector, creating incentives that can favor less regulated actors. At present, no effective standing industry-level framework exists to align responsible conduct. Addressing this gap will require coordinated regulatory and multistakeholder approaches that move beyond individual Company programs.
5. **Affected individuals and communities** may be harmed by irresponsible use of cyber intelligence technologies. The Pall Mall Process highlights the importance of accountability mechanisms that enable credible allegations of misuse to be raised and assessed and that support access to appropriate remedies. NSO does not engage directly with individuals or communities in an operational capacity, but maintains external whistleblowing and reporting mechanisms to support the intake and assessment of credible information, subject to legal and jurisdictional constraints.

6.2 Victims of Serious Crime and Terrorism

Discussions concerning the regulation of cyber intelligence capabilities frequently focus on the risks of misuse and the protection of individual rights but often give less attention to the perspectives of victims of serious crime and terrorism whose safety and rights are also directly implicated. Victims of organized crime, human trafficking, sexual exploitation, terrorism, and other forms of grave harm have a legitimate interest in the effectiveness of lawful investigative tools used to prevent offences, disrupt criminal networks, and bring perpetrators to justice.

NSO have not engage to date with such organizations in an operational capacity. However, NSO recognizes that a balanced regulatory discourse on surveillance and cyber intelligence should take account of these perspectives alongside those of civil society, regulators, and affected individuals. Ensuring that the voices of victims of serious crime and terrorism are represented in policy and regulatory discussions can contribute to a more complete understanding of the public interests at stake, including the rights to life, security, and access to justice.

From NSO's perspective, the inclusion of these voices in broader regulatory and multistakeholder processes – such as those concerned with setting standards, defining legitimate use, and calibrating safeguards – can help ensure that governance frameworks reflect the full range of rights and interests engaged by cyber intelligence technologies. This is a matter for policymakers and regulators to consider in shaping inclusive and balanced approaches to oversight, rather than a role for technology providers to assume directly.

6.3 NSO's Submission to the Pall Mall Process

NSO contributed to the Pall Mall Process consultation with a submission grounded in 2 core realities. First, legitimate state uses of cyber intelligence capabilities not only exist, but are essential for fighting crime and terrorism and are recognized under domestic and international legal frameworks. Second, durable protection against misuse requires institutional frameworks that extend beyond any single Company's – or even a single country`s – internal compliance controls. The Pall Mall Summary Report itself acknowledges legitimate uses while highlighting the challenge of shaping incentives and responding effectively to misuse.

6.4 Core Principles Articulated by NSO

NSO's submission framed responsible practice across the CCIC lifecycle – development, facilitation, purchase, transfer, and use – around four operational principles already reflected in NSO's compliance program:

- **Accountability** – achieved through lawful sales, enforceable contractual restrictions, export control licensing, and the ability to investigate and impose consequences for misuse.
- **Precision** – reflected in target-centric product design, strict purpose limitation, proportionality, and technical and contractual controls governing scope, geography, and duration.
- **Oversight** – supported by layered internal governance, independent external licensing authorities, auditability, and escalation mechanisms.
- **Transparency** – focused on disclosure of principles, policies, and processes rather than operational details that could compromise lawful investigations.

6.5 Proposed Structural Solutions

Beyond principles, NSO's submission proposed structural measures aimed at addressing a persistent weakness across the CCIC ecosystem: the absence of a coherent and predictable international regulatory framework. NSO emphasized that responsible use of cyber intelligence capabilities depends on the existence of clear, enforceable rules that states apply domestically and that are supported by coordinated expectations at the international level. In the absence of such alignment, the ability of legitimate authorities to maintain and use these tools responsibly is undermined, while opportunities for misuse and regulatory arbitrage increase.

Against this backdrop, NSO advocated for the development of complementary international compliance doctrine, including greater coordination of licensing standards, industry certification regimes, independent oversight and audit mechanisms, and global incident reporting and grievance frameworks. These measures are intended to reinforce national systems rather than replace them and to create meaningful, market-wide incentives for responsible conduct at scale.

6.6 Grounding in Operational Experience

NSO's positions are informed by operational experience. NSO's Transparency & Responsibility Reports document how safeguards are implemented in practice, including system configuration aligned with export licenses, immutable audit logs, kill-switch capabilities, structured investigation procedures, and enforcement actions, including customer suspensions and terminations with material financial impact. This experience informs NSO's view of what is achievable under existing regulatory arrangements and where additional structural solutions are required.

6.7 Pall Mall Summary Report Priorities and NSO Alignment

The Pall Mall Summary Report identifies a set of good practices for governments and industry. NSO's existing framework aligns closely with these priorities, as illustrated below:

Priority	Summary Report focus	NSO practices
Accountability	• Strong legal frameworks • Export controls • Enforceable responses to misuse	• Transaction-specific export licensing • Board and committee oversight • Risk-based HRDD • Misuse investigations and enforcement
Precision	• Narrow, lawful, proportionate use • Clear definitions of legitimate use	• Target-centric design • Purpose limitation • Contractual and technical limits • Operator statements
Oversight	• Independent review, auditability and cross-government coherence	• Immutable audit logs • Escalation to senior management and GRCC • Ability to suspend or disable systems
Transparency	• Publication of principles and processes • Whistleblowing • Supplier transparency	• Transparency Reports • Published policies • Internal and external whistleblowing mechanisms • Supplier Code of Conduct

This alignment demonstrates that most of the practices identified as proposed good practice at the international level are already embedded in NSO's operating model. At the same time, the Summary Report underscores that these measures are most effective when supported by broader regulatory and institutional frameworks.

6.8 Export Controls as a Complementary Governance Tool

Export control regimes remain a principal mechanism through which states regulate the transfer of CCICs. In practice, however, existing frameworks vest discretion over authorization decisions in national authorities without a harmonized international standard governing when such exports are legitimate. Experience under regimes such as the Wassenaar Arrangement demonstrates both the value and the limits of export

controls: They can function as effective gatekeepers, but uneven implementation and definitional ambiguity prevent them from establishing a consistent global baseline.

Export controls regulate transfer, not use. They do not provide ongoing oversight of deployment by sovereign end-users or address post-deployment misuse across borders. NSO's operating experience reflects these dynamics. Transaction-specific export authorization is an essential layer of independent oversight, but the absence of shared international criteria means that companies operating under strict regimes may remain exposed to retrospective scrutiny for decisions entrusted to states.

NSO's position is that effective governance requires either clearer international standards to guide authorization decisions across jurisdictions or explicit recognition that export authorization by a competent national authority – following applicable due diligence – constitutes completion of a Company's export-control obligations. Within the limits of its role, NSO seeks to mitigate this gap through rigorous internal due diligence and support for complementary international mechanisms that reinforce, rather than replace, state responsibility.

6.9 NSO's Perspective on the Path Forward

NSO supports the direction reflected in the Pall Mall Process and view that it can be an important step toward greater international alignment. For such efforts to be relevant and effective, they must begin from a clear recognition that the lawful use of cyber intelligence tools is necessary for the prevention and investigation of serious crime and terrorism, and forms part of modern law-enforcement and national-security practice. At the same time, experience shows that voluntary principles must evolve into frameworks capable of changing incentives in a global and unevenly regulated market.

Effective governance in this domain also requires a holistic view of responsibility across the ecosystem. This includes appropriate due diligence by providers of communication, encryption, and related technologies whose products shape the investigative environment and contribute to the "going dark" challenge faced by lawful authorities. Stakeholder engagement is not ancillary to compliance – it is an extension of it. The Company's objective is not merely to meet existing standards, but to contribute to the development of governance frameworks that make responsible practice the norm rather than the exception across the CCIC ecosystem.

7 Looking Ahead: 2026 Commitments

The governance of commercial cyber intrusion capabilities is entering a period of accelerated evolution. Expectations from governments, regulators, civil society, and international bodies are increasingly converging around the need for clearer standards, stronger oversight, and more coordinated responses to misuse. At the same time, democratic states continue to face complex security challenges, with serious crime, terrorism, and hostile activity increasingly exploiting encrypted and anonymized digital environments.

Against this backdrop, NSO Group views 2026 as a period focused on consolidation, alignment, and disciplined implementation. Building on the governance structures, compliance framework, and stakeholder engagement described in this report, NSO has identified a set of priorities to guide its approach in the period ahead.

NSO will continue to engage constructively in multistakeholder initiatives aimed at developing coherent international approaches to the governance of commercial cyber intrusion capabilities. In particular, NSO will support efforts under the Pall Mall Process and related forums to translate high-level principles into clearer definitions and workable expectations for both states and industry. While voluntary initiatives alone cannot resolve all structural challenges in a fragmented global market, they play an important role in building shared understanding, identifying gaps, and informing more durable regulatory and oversight mechanisms.

Internally, NSO will continue to refine its governance, risk management, and oversight arrangements to ensure they remain effective as risk profiles evolve. This includes ongoing review of Board-level oversight, the role of the GRCC Committee, and the independence and resourcing of the Compliance Team. NSO will also assess how technological developments – particularly in areas such as artificial intelligence and automation – may affect both the capabilities of cyber intelligence tools and the associated human rights risk landscape, and will integrate these considerations into product governance and safeguard design where appropriate.

Human rights due diligence will remain a central pillar of NSO's approach. The Company will continue to refine its risk assessment methodologies, calibrate mitigation measures in higher-risk environments, and emphasizes periodic reassessment rather than static approvals. NSO will also continue to review the effectiveness of its contractual and technical safeguards to ensure they remain fit for purpose.

NSO recognizes that accountability depends not only on preventive controls, but also on credible mechanisms for reporting, investigation, and response. In 2026, NSO will continue to operate and, where appropriate, enhance its internal and external whistleblowing mechanisms, investigation procedures, and escalation pathways. While NSO does not seek to replace sovereign oversight or judicial remedies, it supports the development of broader accountability and grievance frameworks as a necessary complement to corporate compliance.

Consistent with its submissions to international processes, NSO will continue to support structural solutions that address the limitations of fragmented national approaches, including greater coordination on licensing standards, exploration of industry certification models, and mechanisms for independent oversight and information-sharing among competent authorities. NSO's engagement on these issues will remain pragmatic and grounded in experience, with the objective of reinforcing – rather than displacing – state responsibility.

Finally, NSO remains committed to transparency as an ongoing practice. The publication of this report reflects that commitment, as does NSO's continued engagement with stakeholders in good faith. NSO will continue to report on the evolution of its governance, compliance program, and enforcement actions, subject to legal and confidentiality constraints, and to participate constructively in policy discussions shaping the future of the cyber intelligence ecosystem.

8 Conclusion

The governance of commercial cyber intrusion capabilities presents complex challenges at the intersection of technology, security, and human rights. These capabilities can play a legitimate and essential role in enabling governments to protect their citizens from serious crime, terrorism, and evolving digital threats. At the same time, their misuse carries real risks to fundamental rights and democratic institutions. Addressing this tension responsibly requires disciplined governance, credible oversight, and coordinated action across the ecosystem.

This report has described how NSO Group approaches that responsibility in practice. It sets out the governance structures, human rights compliance framework, due diligence processes, safeguards, and investigation mechanisms that NSO has developed and operationalized over several years. It also situates those efforts within a broader international context, recognizing that effective accountability in this domain depends not only on Company-level controls, but on coherent legal frameworks, independent oversight, and meaningful collaboration among governments, industry, civil society, and the research community.

NSO's engagement in multistakeholder initiatives, including the Pall Mall Process, reflects a clear understanding that durable solutions must be developed collectively and grounded in operational reality. The alignment between NSO's existing practices and emerging international expectations demonstrates that structured, enforceable approaches to governance are both feasible and necessary – while also underscoring the importance of addressing remaining structural gaps in a fragmented global regulatory landscape.

As the sector continues to evolve, NSO remains committed to acting as a responsible participant within its defined role. This includes maintaining and strengthening internal controls, enforcing consequences when misuse is identified, engaging constructively with stakeholders, and contributing to the development of international frameworks capable of shaping behavior across jurisdictions. It also includes recognizing the importance of clear role delineation and supporting governance models that reinforce, rather than replace, state responsibility.

Accountability in the cyber intelligence domain is not a fixed endpoint. It is an ongoing process that must adapt to technological changes, emerging threats, and evolving societal expectations. NSO views this report as part of that process and reaffirms its commitment to transparency, continuous improvement, and responsible engagement as the global conversation on commercial cyber intrusion capabilities continues.