Security clearances and the regulation of national and domestic security personnel

Robert Rizzi and **Charles E. Borden** advocate changes to existing approaches

In recent years, Western security establishments have been subject to a number of significant security breakdowns, with individuals obtaining and widely disseminating massive amounts of classified information. These breakdowns have highlighted some of the limits of the current security process, both in terms of how information is classified, and the process by which governments determine who may have access to classified information.

In the US, and elsewhere, the core component of the process by which a person is provided access to certain categories of classified information is the 'security clearance'. Initially developed during the second world war, and greatly expanded in the early years of the Cold War, the security clearance process rests on a 'certification model' – at prescribed points in time, an assessment is made of an individual's suitability to receive classified information, and the individual is either 'certified' and receives clearance or is denied. The process focuses on the government's national security interest with little weight given to the individual's personal interest – the ability of an applicant to appeal a denial of a security clearance is fairly limited. This approach, however, has begun to show strains, as the changing nature of both government and information has created new challenges for which the current security clearance system is not optimally designed.

In particular, the expansion in the size of government and the increasing use of private contractors in national security-related activities, coupled with rapid changes in information and communications technology, has resulted in a clearance process that is both too broad and insufficiently reliable. The number of government and government-related positions that require security clearances has exploded over the past couple of decades, despite questions about whether and to what extent many of these positions are likely to encounter classified information. This explosion in the number of security clearances that need to be processed has in turn stretched the resources of those agencies responsible for administering the security clearance regime. At the same time, the computer and communications revolution has expanded the volume of classified information exponentially during the same period, making the consequences of a security breach potentially far more wide-reaching than they were in the past. Put simply, under the current security clearance process, significant resources have to be expended on certifying security clearances for individuals and positions that pose little security risk, and at the same time the risks associated with a potential breach have increased substantially.

Moreover, security clearances have taken on a regulatory role that extends well beyond their original purpose of protecting sensitive information. In effect, the security clearance assessment has become less an inquiry into whether a person is capable of handling specific types of sensitive information and more a determination of whether a person should be allowed to work in government or government-related professions. As a practical matter, the failure to obtain a security clearance can end or significantly damage a person's career, and therefore the individual economic stakes for applicants are substantial. Yet, the present security clearance process provides individuals with little ability to challenge a negative security clearance determination.

A changing landscape

Although the security clearance process has broadly remained unchanged since the 1950s, the landscape in which it operates has changed significantly. The growth in the size of the US government, coupled with an increased tendency to designate positions as requiring a security clearance even where there is little likelihood that they will encounter classified information, has led to a massive increase in the number of security clearance reviews that are performed every year. Indeed, it is estimated that in 2014, 5.1 million individuals, primarily Americans, had security clearances granted by the US government (Fung 2014), including roughly 1.5 million at the Top Secret level, and that the cost of 'vetting' those individuals was approximately $6 billion (ibid). Moreover, attachment of a security clearance to a particular individual increasingly has become a form of government franchise or licence. This licence determines whether or not the individual can serve in a wide range of government positions, as well as in private sector positions that have quasi-governmental functions, regardless of whether the position will require contact with classified information (Rizzi et al., 2015: 24-27). This trend has made a security clearance, especially at the higher levels such as Top Secret, a 'bankable' qualification, and a requirement for working in a large number of fields that may be only tangentially related to national security.

Challenges

The current system has created a one-way ratchet in terms of requiring clearances, and of the corresponding scope of clearance investigations. The result has been delays in performing background checks and the use of third-party contractors to conduct investigations, with a predictable impact on quality. Comprehensive monitoring of individuals with access to classified information is limited, and in some spectacular cases, has proved to be inadequate.

Because a security clearance is required for a range of positions, a denial or revocation of a clearance constitutes a de facto regulatory bar to public service. The American system has developed an elaborate process of implementing denials and revocations of security clearances, using terminol-

ogy borrowed from the legal sphere. For example, security clearance denials for private contractors are 'adjudicated' before 'administrative judges' as part of 'hearings and appeals'. But, in fact, the current review system in many respects bears only a superficial resemblance to due process. As the scale of the security clearance process has expanded, and as the holding of a clearance has increasingly become a prerequisite for government jobs and contracts, there has not been a commensurate increase in the protections afforded to individuals in connection with granting or revoking their clearances. Indeed, the rights of affected individuals with respect to clearance determinations have, if anything, been reduced as a result of deferential judicial doctrines.

A major structural flaw in the current security clearance system is its reliance upon a certification model. Under the original 1953 regulatory scheme, as slightly modernized in the 1995 Executive Order, the scheme depends almost entirely upon standardized procedures to determine whether an individual can be 'cleared' for access to classified information and, if answered in the affirmative, the clearance certifies the individual can have such access going forward, even though neither the government nor the individual knows precisely what information will be involved in the future. Moreover, certification systems generally operate on a 'snapshot' in time, often failing to take into account changes in the certified person or his or her circumstances over time.

As with any certification system, the current approach purports to provide assurance, and to create a presumption of continued validity, once the certificate is issued. Many of the spectacular examples of failures of the system involve individuals who may have at one point been deemed sufficiently trustworthy, but became dangerously unreliable, as the result of a variety of changing factors, such as financial distress.

Risk-based reforms?

One possible approach to reforming the current security clearance system would be to rely upon a risk-based personnel evaluation system, which would emphasize ongoing compliance and monitoring, rather than a single certification. A risk-based approach would provide a more comprehensive set of categories of individuals with contact with classified information to replace the three basic categories now used. Such an approach would concentrate resources on those positions as to which individuals would be most likely to handle, or be exposed to, classified information, particularly classified information that creates significant national security risk, and would focus on comprehensively mitigating that risk. In practice, this approach would mean reversing the one-way ratchet, with fewer positions requiring any form of clearance, and with those positions requiring clearance being risk-weighted at the outset. In implementing this approach, it should be possible to measure actual and probable contact between the individual's position and classified information, and to apply more rigorous standards to those with greater access. For example, an individual acting as a systems administrator or maintenance worker with broad access to classified information through highly sensitive IT systems would be subject to the most rigorous standards, regardless of title or seniority. The risk assessment thus would be based on current and probable future activities of the individual, rather than seniority of position.

Furthermore, a reformed compliance and monitoring model could modify or replace a half-century old certification system. Especially for positions that have access to particularly sensitive information, frequent and random reporting and responses to selected inquiries (for example, questions concerning unusual changes in financial holdings or transactions) could provide deterrence from inappropriate conduct with respect to such information. Similar models have been developed in the past to address analogous conduct risks, for example, testing regimes for restricted substances and drugs (for recipients of government licences and airline pilots), and for monitoring potential financial conflicts of interest. These regimes also tend to create and reinforce norms of conduct that reinforce the regulatory regime, because of the periodic reminders that the individual is subject to a special set of rules.

References

Cabinet Office (2013) 'Government security classifications, April 2014.' London: Cabinet Office. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf> Accessed day, month, year.

Fung, B. (2014) '5.1 million Americans have security clearances', *Washington Post*, 24 March 2014. <https://www.washingtonpost.com/news/the-switch/wp/2014/03/24/5-1-million-americans-have-security-clearances-thats-more-than-the-entire-population-of-norway/> Accessed 27 October 2016.

National Counterintelligence and Security Center (2015) '2015 Annual Report on Security Clearance Determinations.' Washington DC: Office of the Director of National Intelligence. <http://www.fas.org/sgp/othergov/intel/clear-2015.pdf> Accessed 27 October 2016.

Rizzi, R., Borden, C. and Holman, D. (2015) 'Ethics regulation of government contractors.' *risk&regulation* (winter): 24–7. <http://www.lse.ac.uk/accounting/CARR/publications/CARRmagRR30---PDF-Version.pdf>

Robert Rizzi is partner at Steptoe & Johnson LLP and **Charles Borden** is partner at Allen & Overy and a **carr** visiting fellow.