OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

Senior Special Forces Identities Exposed Online as MOD Launches Security Review

July 21, 2025

— *Categories: Defence & Security*

A serious breach has come to light: the names and deployment details of at least 20 British Special Air Service (SAS) personnel were publicly accessible online for over a decade due to a Ministry of Defence (MoD) security lapse. The incident has prompted urgent internal reviews into defence data-sharing practices and reassurances over safeguarding sensitive information.

It has emerged that an in-house magazine produced by the Grenadier Guards regimental association published the identities and coded assignments, such as the ‘MAB’ reference to United Kingdom Special Forces headquarters, of at least twenty SAS operatives. These details remained available online despite prior warnings. The publication was updated in 2024, meaning some named individuals may still be serving in operational roles.

Defence Secretary John Healey and Army Chief General Sir Roly Walker reacted forcefully, ordering an immediate investigation. Walker has directed a full review of data-sharing arrangements with all affiliated regimental and corps associations to establish firm protections and guidelines. The Grenadier Guards’ association has since been barred from distributing physical copies and instructed to remove all sensitive content.

The breach follows a separate Ministry of Defence error in which a spreadsheet containing personal details of over 100 British intelligence and special forces personnel, including MI6 officers and SAS members, as well as nearly 19,000 Afghan nationals seeking relocation, was circulated in error. That leak was kept under a super-injunction for around two years before the courts allowed disclosure.

The exposure is widely regarded as one of the most damaging security incidents in recent memory, endangering both personnel and intelligence integrity. Government sources emphasise the paramount importance of protecting lives across all tiers of the security services.

From a centre-right perspective, the lapse is deeply troubling; it undermines the credibility of the Armed Forces and intelligence services

at a time when global threats are escalating. Ministerial and military leadership must deliver swift remedies and demonstrate accountability. Maintaining robust command structures and sourcing protocols is essential to preserving national defence readiness and international standing. The Treasury and the MoD must fund training and technical solutions to manage sensitive data securely, especially in collaboration with external or veteran associations.

The inquiry should result in enforceable policies, mandatory digital safeguards, and regular audits of all affiliated publications. Transparency with Parliament's Intelligence and Security Committee following the super-injunction wrap-up was too slow; future failures are not an option. With inquiry underway, the Ministry must act decisively to restore confidence that the UK's elite forces, and those who support allies abroad, are properly shielded.