Avoiding too much security

# Avoiding too much security

This guidance applies to developers and system administrators who work for the Ministry of Justice (MoJ).

Is it possible to have too much security? Yes. Providing too much security for things or information that do not need protection is a waste of resources. It undermines the value of the security for things that do need it.

[Security by obscurity](https://en.wikipedia.org/wiki/Security_through_obscurity) is one of the weakest approaches for protecting something. It's far better to have a technical control in place to protect the system.

## Not all domain names or IP addresses in Government systems are sensitive items

An example is a domain name or IP address. These values do not need to be secret for all systems. Only those that need it. It might be tempting to say that 'all IP addresses are OFFICIAL-SENSITIVE. This is then used as a reason for an (in)action, such as "I can't email you that network diagram because it contains IP addresses." But the statement has wider consequences. It imposes a set of security requirements for everyone. It imposes them irrespective of the actual secrecy required.

OFFICIAL-SENSITIVE is not a different classification to OFFICIAL. It doesn't need special technical controls or procedures. Rather, it's a reminder to look after a piece of information. It's not a controls checklist. Using labels too casually conflicts with the idea of thinking about information and what we're doing with it, and using that to decide how best to secure the information.

Of course, you might need to keep the access details for some systems secure. An example might be where you cannot maintain or patch a legacy system. But these should be exceptional or 'edge' cases.

There are only a small number of situations where you need to protect IP addresses or domain names. It's usually where the context makes the information sensitive in some way. IP addresses can be personally-identifiable information. For example, a system log file might hold the IP address of a client accessing the system. This might reveal a link between an individual and their use of MoJ services. But the IP address of a public sector server or a router should not be personal data.

Remember also that within the MoJ, system almost always have [RFC1918](https://tools.ietf.org/html/rfc1918) addresses. These are normally not routable from the Internet. If you can access the system from the Internet, then you have other problems to resolve. Address them by appropriate security measures rather than hoping that secrecy is enough.

In other words, avoid saying that 'all IP addresses and domain names must be secure'. Instead, think about and justify the handling protections around each piece of information. Ask what data or capability is actually in need of protection, and from what risks.

## It's not only about domain names or IP addresses

The need to keep some aspect of a system secret might be evidence that the technical security measures around the system are not complete, adequate, or appropriate to the risks. A well-designed system won't depend on secrecy alone for security.