DOSR/RN/2026-05 – Radiofrequency Directed Energy Weapons Compliance Guide

Date: 30 MAR 26

Purpose

1. This document provides guidance on the compliance landscape applicable to Radiofrequency Directed Energy Weapon (RFDEW) systems and activities.

2. It is intended to support Accountable Persons and delivery organisations in identifying and navigating relevant legislative, regulatory and policy requirements associated with the procurement, integration, trial, operation, maintenance, and disposal of RFDEW capabilities.

3. The document signposts key sources of compliance obligation and recognised good practice. It does not create new regulatory requirements and does not replace the need for professional judgement, formal safety assessment, or legal advice.

Scope

4. This guidance applies to RFDEW systems and activities conducted by or on behalf of Defence, including research, development, trials, training, operational use, and disposal.

5. It addresses the management of risks arising from electromagnetic emissions, system integration, and operational use, including potential impacts on personnel, third parties, equipment, and the environment.

Approach

6. RFDEW systems operate within a complex compliance landscape comprising statutory legislation, Defence regulation, policy, and recognised standards.

7. This document adopts a structured approach to help users identify which elements of that landscape may be relevant to a given system or activity. Not all requirements described in this document will apply in all cases. The Accountable Person remains responsible for determining applicability and demonstrating compliance proportionate to the hazards and risks presented.

Context

8. RFDEW systems could be considered a subset of Electronic Attack capability. However, within current Defence structures and governance arrangements, RFDEW systems are typically treated as distinct from Electronic Warfare systems, jamming systems, and conventional radiofrequency transmitters such as communications equipment and radar.

9. The boundaries between these domains are not always clearly defined and reflect established organisational and policy arrangements rather than clear technical distinctions.

10. For the purposes of this document, systems designated as RFDEW are considered within the compliance landscape described herein. Systems classified under alternative domains may be subject to different compliance routes and are outside the scope of this guidance.

How to Use This Guide

11. This document is intended as a signposting and orientation tool rather than a prescriptive checklist. It should be used to support understanding of the compliance landscape and to guide the development of a structured compliance argument.

12. Users should begin by identifying the system or activity under consideration and the associated hazards. This guide can then be used to identify relevant areas of legislation, regulation, and policy that may apply. These should be considered alongside established Defence safety management processes, including hazard identification, risk assessment, and safety case development.

13. This guide is not exhaustive and does not remove the need for professional judgement. The Accountable Person remains responsible for determining which requirements apply and for demonstrating that those requirements have been met.

Overview of the Compliance Landscape

14. The compliance landscape for RFDEW systems spans multiple regimes that must be considered in combination. These include requirements relating to electromagnetic field exposure, control and authorisation of spectrum use, and the broader safety management of systems and activities.

15. Effective compliance requires that these domains are not treated in isolation but are addressed collectively as part of a coherent safety and assurance approach.

Statutory Legislation

16. RFDEW systems and activities are subject to applicable UK legislation. This includes legislation governing health and safety, electromagnetic field exposure, and the use of the electromagnetic spectrum. Key legislation includes:

a. Health and Safety at Work etc. Act 1974 (HASAWA)

b. Management of Health and Safety at Work Regulations 1999 (MHSWR)

c. Control of Electromagnetic Fields at Work Regulations 2016 (CEMFAW)

d. Wireless Telegraphy Act 2006 (WTA)

e. Provision and Use of Work Equipment Regulations 1998 (PUWER)

f. Electromagnetic Compatibility Regulations 2016 (EMC Regulations)

g. Environmental Protection Act 1990 (EPA)

17. Depending on the system and operating context, additional legislation relating to environmental protection, communications infrastructure, or product safety may also be applicable.

18. While legislation defines the duties that must be met, it does not prescribe how compliance should be structured or demonstrated. Within Defence, compliance is expected to be explicit, evidence-based, and auditable.

Defence Regulation

19. RFDEW systems fall within the scope of Defence Safety Authority (DSA) regulation, including DSA 02.OME: Defence Ordnance, Munitions and Explosives (OME) Regulations.

20. These regulations define expectations for the management of system safety, including the identification of hazards, implementation of controls, and provision of assurance. Compliance with regulations such as 101: OME Design Requirements, and 105: Safety Risk Management will play a key role in providing assurance of safe RFDEW systems. Electromagnetic hazards should be addressed alongside other hazards within a coherent and integrated safety case.

21. Other, domain-specific, regulations may also apply.

Defence Policy and Safety Frameworks

22. Defence policy provides the framework within which statutory duties are implemented and demonstrated. This framework is composed of general safety policy, acquisition and risk management policy, and policy relevant to electromagnetic emissions. Core Defence safety and risk management policy includes:

a. JSP 375: Management of Health and Safety in Defence

b. JSP 376: Defence Acquisition Safety Policy

c. JSP 815: Defence Safety Management System

d. JSP 816: Defence Environmental Management System

23. These documents define how safety is managed across Defence, including expectations for hazard identification, risk assessment, governance, assurance, and documentation. They establish the processes by which compliance with legislation is demonstrated through structured safety arguments and supporting evidence and maintained throughout the lifecycle of a system or activity.

24. In addition to these general frameworks, RFDEW systems are subject to domain-specific policy relating to the use of the electromagnetic spectrum and the control of electromagnetic radiation. This includes:

a. JSP 392: Management of Radiation Protection in Defence, Chapter 35 Electromagnetic Fields 0 Hz – 300 GHz (Including Radio Frequency Radiations)

b. JSP 453: Digital Policies and Standards for Defence, Defence Electromagnetic Authority Standard

25. These policies provide specific direction on the control, coordination, and safe use of electromagnetic emissions, including requirements for spectrum authorisation and the management of exposure risks.

26. The Accountable Person should apply these policies in combination. General Defence safety policy defines how risks are identified, assessed, and managed, while RF-specific policies define constraints and controls associated with electromagnetic emissions. Together, they provide the basis for a coherent and demonstrable approach to compliance.

Standards and Technical Guidance

27. Recognised standards and technical guidance are used within Defence to support the assessment and control of electromagnetic field exposure and to demonstrate compliance with statutory requirements. Their application should be proportionate to the characteristics of the system and context in which it is used.

28. For RFDEW systems, this includes the application of internationally recognised exposure limit frameworks, as set out in JSP 392. These standards provide established limits and methodologies for evaluating electromagnetic field exposure and are used to inform risk assessment and control measures. Applicable standards include:

a. **ICNIRP 1998 Guidelines**[1] establish the general public exposure limits. ICNIRP published updated guidelines in 2020, and while not reflected in CEMFAW 2016, Ofcom recognises the updated guidelines as the current scientific benchmark[2].

b. **IEEE C95.1-2345-2014**[3] has been implemented by the MOD for the assessment of exposure and exposure limits for “Workers” to electromagnetic fields, exercising a derogation within CEMFAW 2016.

c. **CENELEC CLC/TR 50427:2004**[4] applies to the assessment of inadvertent ignition of flammable atmospheres.

d. **Def Stan 05-074**[5] contains the preferred means of compliance with statute and JSP 392.

29. In addition, recognised standards and methods for hazard assessment should be applied to determine exposure zones, assess potential exposure scenarios, and support the identification of appropriate controls to enable consistent, evidence-based assessment of RF hazards.

---

[1] International Commission for Non-Ionising Radiation Protection 1998 Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields (up to 300 GHz)
[2] Guidance on EMF Compliance and Enforcement, Ofcom, 9 February 2026.
[3] Standard for Military Workplaces--Force Health Protection Regarding Personnel Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz
[4] Assessment of inadvertent ignition of flammable atmospheres by radio-frequency radiation. Guide
[5] Guide to Practical Safety Aspects of the Use of Radio Frequency Energy - Issue 4: 02/2025

Spectrum Management and Emissions Approval

30. The use of RFDEW systems by the MOD is subject to Defence spectrum management policy and associated emissions control processes.

31. Within this framework, the Defence Spectrum Policy team is responsible for setting MOD policy on the use of electromagnetic spectrum and leading international engagements which govern global spectrum cooperation. The Defence Electromagnetic Authority (DEMA) is responsible for the coordination and approval of Defence-related electromagnetic emissions within the UK and overseas, along with providing advice and guidance to teams in relation to emissions and Electromagnetic Environmental Effects (E3).

32. The use of electromagnetic spectrum in the UK is subject to statutory regulation, with Ofcom acting as the national regulator. Within Defence, engagement with Ofcom and management of spectrum use is conducted through DEMA. RFDEW users do not engage directly with Ofcom but should recognise that emissions approval operates within this wider regulatory framework.

33. At present, RFDEW emissions are managed through processes developed for Electronic Attack and jamming systems, including the Procedure for the Control of Non-Operational Jamming (PCNOJ) process. This provides a mechanism for authorising emissions within defined parameters such as location, frequency, and duration.

34. These arrangements form part of a broader spectrum management regime and operate alongside the safety and risk management frameworks described above. Compliance with spectrum policy and emissions approvals processes is therefore a necessary but distinct aspect of demonstrating overall compliance.

35. It is recognised that RFDEW systems may not align fully with the assumptions underpinning existing jamming processes. However, a distinct approval framework for RFDEW has not yet been established. Engagement with DEMA and relevant spectrum authorities at an early stage is therefore essential to ensure that appropriate approval routes are identified and that constraints associated with spectrum use are understood and incorporated into planning, system development, and safety assessment.

Supplier-Led Development, Trials, and Spectrum Regulation

36. The Defence spectrum management policies and DEMA processes apply to RFDEW activities conducted under MOD authority or within MOD-controlled environments.

37. Where industry partners undertake development, testing, or trials outside MOD control, they remain subject to statutory regulation, including requirements imposed by Ofcom as the UK spectrum regulator. In such cases, Defence spectrum policy and approval processes do not apply directly, and suppliers are responsible for obtaining any necessary permissions to use the electromagnetic spectrum.

38. This distinction can cause practical challenges where activities transition between industry-led development and MOD-led trials or use.

39. Early engagement with MOD and relevant regulatory authorities is important to ensure that appropriate approval routes are identified and that activities can be conducted lawfully, particularly where existing regulatory frameworks or processes do not align with the characteristics of RFDEW systems.

Authority and Accountability

40. RFDEW systems and activities span multiple compliance regimes, each with different authorities, responsibilities, and approval mechanisms. There is no single authority responsible for all aspects of RFDEW compliance.

41. The Accountable Person remains responsible for the identification, assessment, and control of risks associated with RFDEW systems and activities. Approval, coordination, or authorisation by other authorities does not transfer ownership of risk.

42. Different authorities set policy, provide regulatory oversight, and grant approvals within their respective domains. These functions support compliance but do not replace the need for the Accountable Person to form and justify a view on risk.

43. For practical purposes, each compliance theme has a primary interface within Defence, supported by additional regulatory or policy authorities. The Accountable Person should ensure that all relevant interfaces are identified and engaged as appropriate.

44. Table 1, below, provides an overview of how accountability, policy and regulatory authority, and coordination and approval responsibilities are distributed across RFDEW activities.

Table 1: Summary of Accountability and Authority Distribution Across RFDEW Areas

Function / Decision Area	Primary Risk Owner	Policy / Regulatory Authority	Acceptance / Approval Authority
System safety (design, integration, hazards)	Accountable Person	DDS, DOSR	DOSR
Electromagnetic exposure safety (personnel and public)	Accountable Person	DDS	DEMA
Spectrum use and emissions	Accountable Person	Defence Spectrum Policy	DEMA
Electromagnetic Compatibility / Interference	Accountable Person	Defence Spectrum Policy	DEMA
Activity planning and execution	Accountable Person	DDS, DOSR	DEMA, Range Authorities
Industry-led development and trials	Supplier / organisation conducting activity	HSE, Ofcom	Ofcom

Key Compliance Themes for RFDEW

45. RFDEW systems must be managed across compliance themes that arise throughout the system lifecycle, from design and integration through to trials, operation, and disposal. These themes do not introduce new requirements but provide a structured way of identifying how different legislative requirements, Defence policy, and technical standards apply in combination.

46. Table 2, below, provides an indicative mapping of key compliance themes to the legislation, Defence policy, and standards that are typically relevant. It is intended as a guide to help identify applicable requirements and is not exhaustive.

47. For the purposes of this section, protection of personnel and third parties refers specifically to risks arising from exposure to electromagnetic fields generated by RFDEW systems. Other hazards associated with weapon systems are addressed through applicable Defence policy and safety regulations and are not the focus of this guidance.

Table 2: Summary Mapping of Compliance Themes to Legislative, Policy, and Regulatory Drivers

Theme	Legislative Drivers	Defence Policy and Regulation	Standards / Technical Basis
Protection of Personnel	HASAWA, CEMFAW	JSP 392	IEEE C95.1-2345
Protection of Third Parties	HASAWA	JSP 392	ICNIRP 1998
Off-Range and Collateral Effects	HASAWA, EPA, WTA (interference and spectrum use), EMC Regulations	JSP 453 DEMA Standard	CLC/TR 50427
System and Platform Integration	HASAWA, PUWER, EMC Regulations	JSP 392, JSP 453 DEMA Standard, DSA 02.OME	Def Stan 59-411 Def Stan 59-114 Def Stan 07-085
RFDEW Activity Planning and Execution	HASAWA, MHSWR, WTA (lawful spectrum use)	JSP 375, JSP 376, JSP 815, JSP 816, DSA 02.OME	

Protection of Personnel

48. A primary safety consideration for RFDEW is the exposure of personnel to electromagnetic fields generated by RFDEW systems.

49. Assessment should determine whether personnel may be exposed above applicable limits during operation, maintenance, testing, or fault conditions. This should take account of system characteristics such as power, frequency, directionality, and duty cycle. Where personnel may be present within areas of potential exposure, the Accountable Person must ensure that risks are assessed and controlled so far as reasonably practicable.

50. This theme is driven by HASAWA and CEMFAW, with JSP 392 setting out Defence policy. The MOD has adopted the IEEE C95.1-2345-2014 exposure limits for MOD personnel.

51. This theme applies throughout the lifecycle, including development, trials, operation, maintenance, and disposal. Compliance is typically demonstrated through hazard identification, exposure assessment, and the implementation of controls within the Defence safety management framework.

Protection of Third Parties

52. RFDEW activities may present risks to individuals who are not directly involved in the operation of the system, including members of the public, personnel in adjacent areas, and other third parties.

53. This theme also requires consideration of individuals who may be more susceptible to electromagnetic effects, including those using medical or assistive devices such as wearable or implanted medical devices or life-supporting equipment.

54. This theme is primarily driven by HASAWA, with JSP 392 setting out related Defence policy including implementing the third-party exposure limits in ICNIRP Guidelines.

55. This theme is particularly relevant during trials and operational use where emissions may extend beyond controlled areas. Compliance requires consideration of reasonably foreseeable exposure scenarios and the implementation of controls to prevent harm.

Off-Range and Collateral Effects

56. RFDEW systems may produce effects beyond the immediate operating area, where electromagnetic energy interacts with infrastructure, equipment, or the environment. This includes the potential for disruption, degradation, or damage to electronic systems, communications, sensors, or other equipment, including systems owned or operated by third parties. Such effects may arise through direct propagation, reflection, or coupling into systems or structures.

57. This theme is distinct from the protection of persons and focuses on the impact of RF emissions on systems and infrastructure. However, such effects may have safety implications where affected systems perform critical or life-supporting functions.

58. Assessment should also consider potential contingent liability arising from damage or disruption, in accordance with the HM Treasury Contingent Liability Approval Framework and applicable MOD processes.

59. Compliance requires consideration of how RF energy behaves outside the intended operating envelope and whether it may affect systems beyond the control of the operator, including identification of reasonably foreseeable interaction mechanisms and implementing appropriate controls or constraints.

60. This theme is particularly relevant during trials and operational use, where off-range effects may influence both safety controls and approval conditions, and where wider disruption to civilian infrastructure, services, or commercial activities may give rise to societal or stakeholder concerns.

System and Platform Integration

61. Where RFDEW systems are integrated into platforms, compliance must address the interaction between the RFDEW system and other platform systems.

62. In the context of this document, this theme is primarily driven by HASAWA, PUWER and the EMC Regulations, supported by JSP 392, JSP 453, and DSA 02.OME Regulations.

63. Compliance requires that RF hazards, including electromagnetic compatibility and interference, are considered as part of the overall system safety case. This theme is most relevant during design, integration, and modification of systems.

RFDEW Activity Planning and Execution

64. The safe and compliant use of RFDEW systems depends on the effective integration of multiple compliance domains during planning and execution activities.

65. In addition to general Defence safety management requirements, RFDEW activities require coordination of:

a. System safety considerations, including hazards to personnel and third parties.

b. Spectrum management and emissions approval.

c. Off-range and collateral effects, including potential impacts on infrastructure and services.

d. Any associated contingent liability and societal considerations.

66. These factors are interdependent and should be addressed in combination when defining how an activity will be conducted.

67. This theme is particularly relevant during trials and non-operational use, where activities must be explicitly planned, authorised, and coordinated across multiple stakeholders. Early engagement with relevant authorities, including safety, spectrum, and range or site management functions, is essential to ensure that constraints are understood and that appropriate controls are implemented.

68. During execution, activities should be conducted within the defined constraints and assumptions used to support safety and approval. Where conditions change, or where assumptions are no longer valid, activities should be reviewed and, where necessary, modified or stopped.

Interfaces and Dependencies

69. RFDEW compliance is dependent on effective coordination across multiple domains.

70. These include range safety, platform safety, environmental management, and spectrum management. In many cases, the safe and compliant operation of an RFDEW system will depend on the alignment of controls and approvals across these domains.

71. The Accountable Person should ensure that relevant interfaces are identified and managed, and that dependencies are understood and addressed as part of the overall safety approach.

Limitations of This Guide

72. This document provides guidance on the compliance landscape for RFDEW systems and activities but does not constitute a complete or authoritative statement of all applicable requirements.

73. This guide does not replace statutory obligations, Defence regulation or policy, or formal safety assessment processes. It should not be used as a substitute for legal or specialist technical advice.

74. The Accountable Person remains responsible for determining applicability and demonstrating compliance.

Queries

75. Any observations or requests for further guidance on the content of this DRN should be submitted by email to dsa-dosr-prg@mod.gov.uk.

Stephen A. Gillstroem McLean, MIEXPE, PIEMA
DOSR TL